Citrix Workspace-App für iOS

Contents

Info zu diesem Release

January 15, 2021

Neue Features in EAR Build 21.1.0

iOS-Versionsunterstützung

Citrix Workspace-App 21.1.0 für iOS ist das aktuelle Release, das iOS Version 10.x unterstützt.

Neue Features in Release 20.12.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.11.0

Erweiterte Webansicht mit nativen Steuerelementen für SaaS-Apps

Mit dieser Version können Sie eine erweiterte Webansicht mit nativen Steuerelementen für SaaS-Apps verwenden. Diese Erweiterung ermöglicht Folgendes:

- Anzeigen der URL Ihrer Apps.
- Anzeigen der Sicherheitsinformationen Ihrer Apps.
- Teilen von Apps.

Außerdem können Sie Ihre Apps jetzt nach links und rechts streichen, um vorwärts bzw. rückwärts zu navigieren.

Neue Features in Release 20.10.5

Unterstützung für Sondertasten

Diese Version bietet Unterstützung für die folgenden Tastenkombinationen auf externen iOS-Tastaturen hinzu:

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M

- Windows + S
- Windows + STRG + S
- Windows + T
- Windows + U
- Windows + Nummer
- Windows + Aufwärts
- Windows + Abwärts
- Windows + Nach links
- Windows + Nach rechts
- Windows + X
- Windows + K
- STRG + ESC

Neue Features in Release 20.10.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.9.5

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.9.0

Externe Freigabe von Webseiten

Ab diesem Release können Sie die Webseiten, die Sie über die Citrix Workspace-App für iOS öffnen, für andere freigeben. Sie haben folgende Möglichkeiten:

- Link aus einer Webansicht kopieren
- Webseite direkt in Safari öffnen
- Links direkt an Personen oder Apps senden

Tippen Sie dazu auf das Symbol **...** oben rechts in der Webansicht oder tippen Sie lange auf einen beliebigen Link in der Webansicht und tippen Sie dann auf die gewünschte Option.

Neue Features in Release 20.8.1

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.8.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.7.6

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.7.5

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.7.0

Unterstützung für externen Bildschirm und Symbolleiste

Das Feature für den externen Bildschirm und die Symbolleiste ist jetzt allgemein verfügbar. Diese Version umfasst auch Fehlerbehebungen in Bezug auf dieses Feature.

Unterstützung für generische Mäuse und Trackpads

Ab diesem Release können Sie eine generische Maus oder ein Trackpad verwenden, um in HDX-Sitzungen mit der rechten Maustaste zu klicken, zu scrollen und den Mauszeiger zu verwenden. Die Aktionen ähneln denen der Citrix X1-Maus. Der Stil des lokalen Mauszeigers ändert sich und gleicht dem des Remotecursors.

> **Hinweise:**
>
> - Dieses Feature ist auf iPadOS 13.4 und höher verfügbar.
> - Dieses Feature wird auf iPhones nicht unterstützt.

Einschränkung:

Wenn Sie während einer Sitzung einen externen Monitor anschließen, bleibt der generische Mauszeiger aufgrund einer iOS-Einschränkung auf dem nativen Gerät.

Unterstützung für mehrstufige Authentifizierung (nFactor)

Die mehrstufige Authentifizierung erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten. Mit der mehrstufigen Authentifizierung können Authentifizierungsschritte und die zugehörigen Anmeldeinformationsformulare vollständig vom Administrator konfiguriert werden.

Die native Citrix Workspace-App kann dieses Protokoll über die unterstützten Anmeldeformulare nutzen, die bereits für StoreFront implementiert sind. Die webbasierte Anmeldeseite für virtuelle Citrix Gateway- und Traffic Manager-Server verwendet ebenfalls dieses Protokoll.

Weitere Informationen finden Sie unter SAML-Authentifizierung und Mehrstufige Authentifizierung (nFactor).

Einschränkung:

Wenn die Unterstützung für mehrstufige Authentifizierung (nFactor) aktiviert ist, können Sie keine biometrische Authentifizierung, wie Touch ID und Face ID, verwenden.

Unterstützung für Sondertasten

Dieses Release bietet Unterstützung für die folgenden Einzeltasten auf einer externen Tastatur ab iOS 13.4 und höher:

- Bild-auf
- Bild-ab
- Pos1
- Ende
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

Neue Features in Release 20.6.0

Unterstützung für externen Bildschirm und Symbolleiste Featurevorschau

Ab diesem Release können Sie die Citrix X1-Maus verwenden, um die Symbolleiste auf einem externen Bildschirm zu bedienen. Sie können die Symbolleistenverankerung nun auch horizontal verschieben, während die Symbolleiste geschlossen ist. Wenn Sie Ihr iOS-Gerät mit dem externen Bildschirm verbinden, erkennt die Citrix Workspace-App automatisch die Bildschirmauflösung des externen Bildschirms. Sie können die Schaltfläche **Anzeige** in der Symbolleiste verwenden, um eine bestimmte Bildschirmauflösung auszuwählen. Sie können auf die Option **Anzeige** zugreifen, ohne vorher ein Konto hinzufügen oder sich anmelden zu müssen.

Neue Features in Release 20.5.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.4.5

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

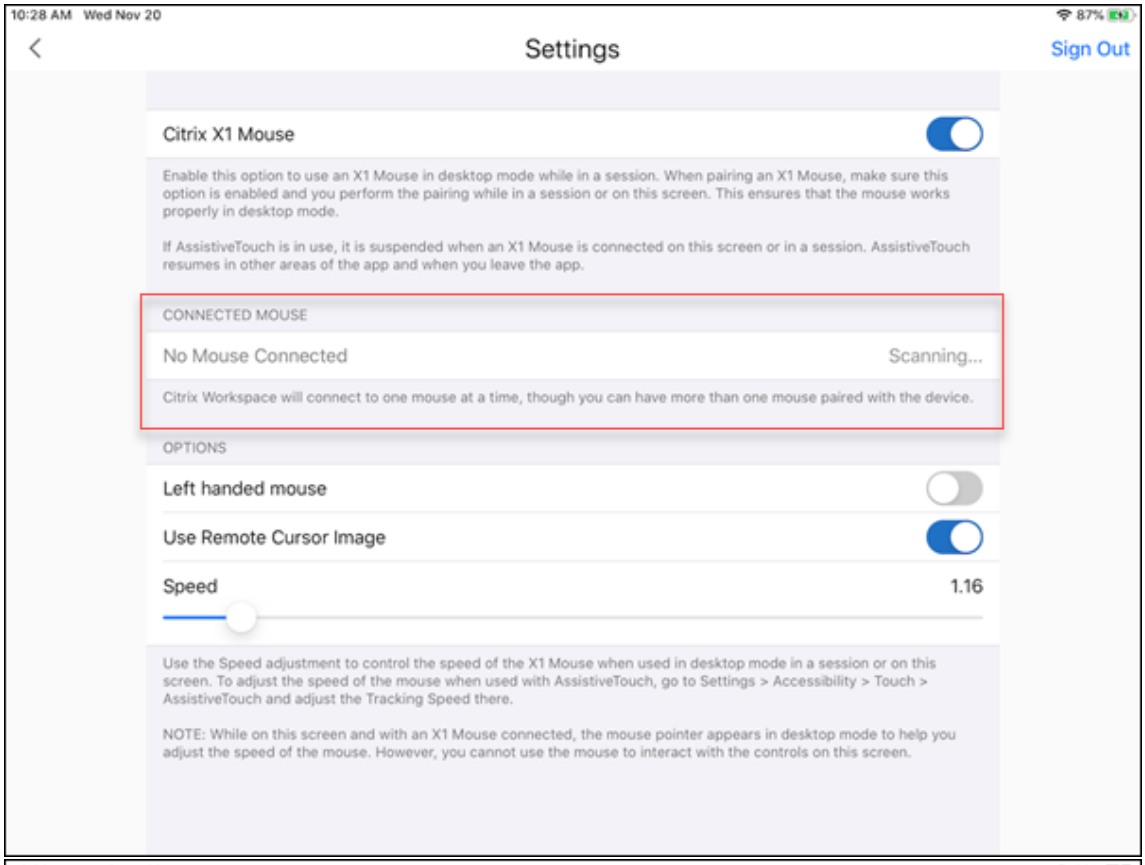
Neue Features in Release 20.4.0

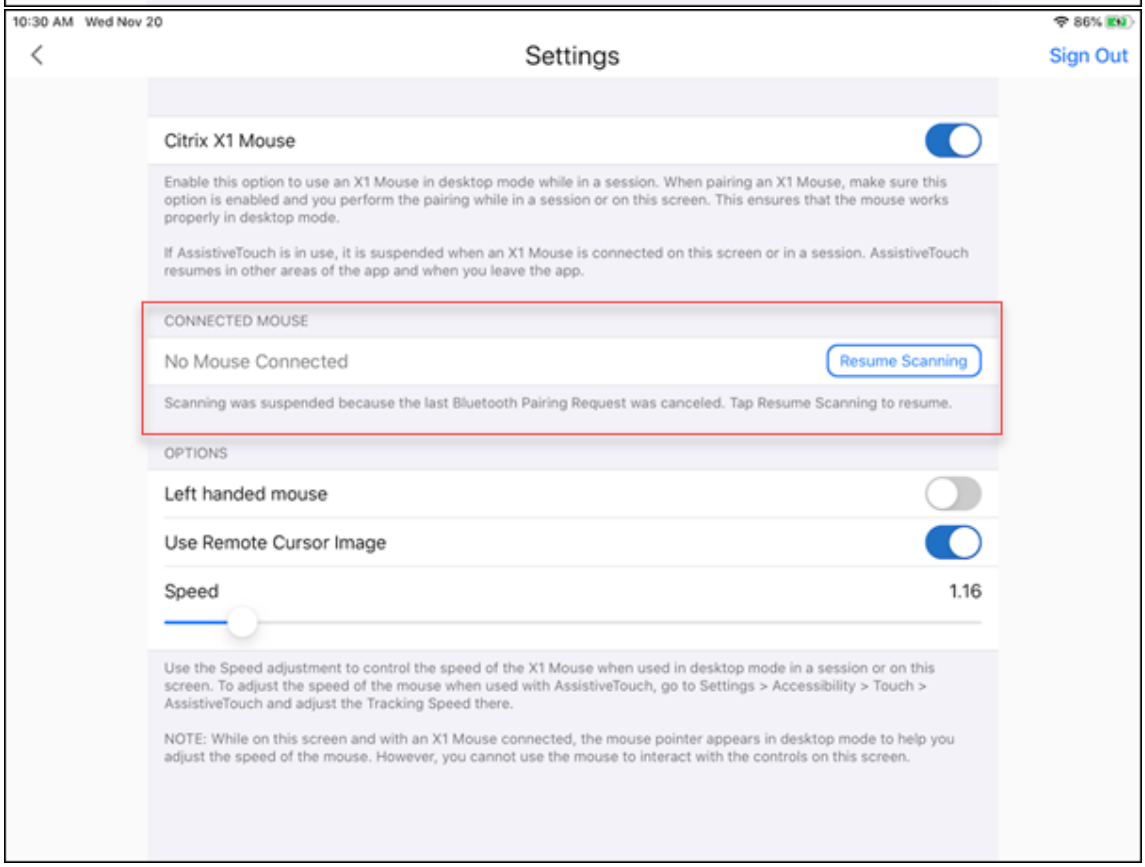
> **Hinweis:**
>
> Ab Juni 2020 unterstützt die Citrix Workspace-App iOS-Versionen 11.x nicht mehr. Alternativ können Sie Ihr iOS-Betriebssystem auf Version 12 oder höher aktualisieren.

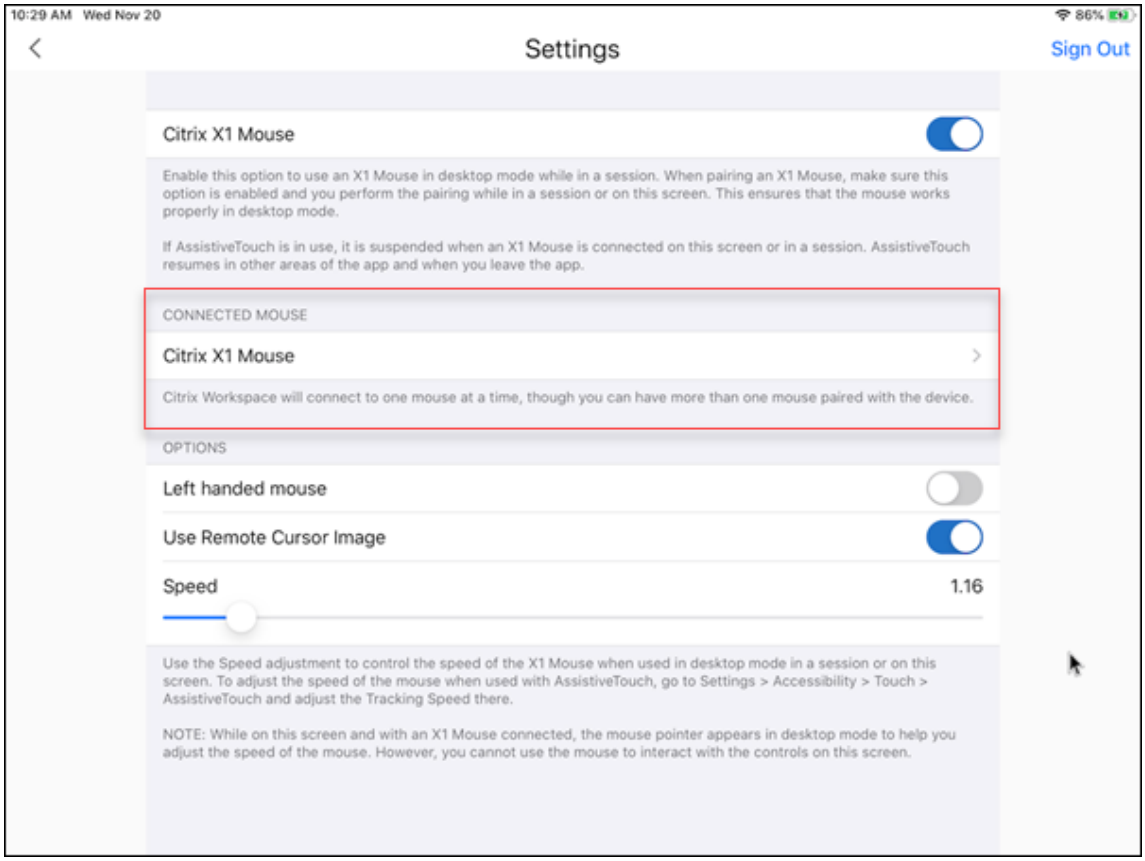
Citrix X1-Mauskopplung und Verbindungsstatus

Mit dieser Funktion haben Sie mehr Kontrolle über den Kopplungsprozess der Citrix X1-Maus. Der Bildschirm **Einstellungen** bietet folgende Optionen:

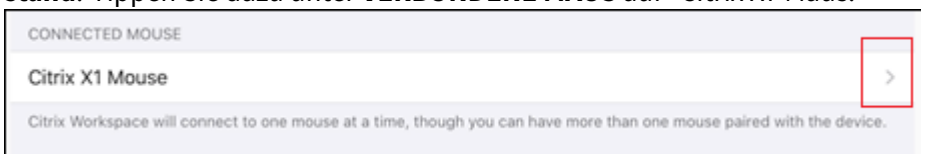
- Koppeln der Citrix X1-Maus. Sie können eine X1-Maus auch koppeln, wenn Sie in einer Sitzung sind.
- Anzeigen des Verbindungsstatus.







- Anzeigen von Eigenschaften der Citrix X1-Maus, z. B. **Name**, **UUID**, **Firmwareversion**und **Akkustand**. Tippen Sie dazu unter **VERBUNDENE MAUS** auf “Citrix X1-Maus.



Eigenschaften der verbundenen Maus:

AssistiveTouch

Wenn die AssistiveTouch-Funktion unter iOS 13 oder höher aktiviert ist, können Sie den AssistiveTouch-Cursor sehen, wenn Sie zwischen Desktopmodus und AssistiveTouch-Modus wechseln.

> **Hinweis:**
>
> Im Desktop-Mausmodus wird der Zeigercursor angezeigt. Im AssistiveTouch-Modus wird der runde Cursor angezeigt.

Der AssistiveTouch-Cursor wird in folgenden Fällen angezeigt:

- Beim Verlassen einer Sitzung
- Beim Wechseln zum iOS App Switcher-Bildschirm
- Beim Wechseln zum iOS-Startbildschirm oder zu einer anderen App

Der Desktopmodus wird fortgesetzt, wenn Sie zurück zur Citrix Workspace-App navigieren und wenn Sie in einer Sitzung sind.

Neue Features in Release 20.3.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.2.2

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.2.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.1.5

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Release 20.1.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme

Behobene Probleme in Release 21.1.0

Auf iPads, die unter iOS 13 oder höher ausgeführt werden, werden SaaS-Apps möglicherweise im sicheren Browser geöffnet, selbst wenn die Einstellung **Enforce policy on mobile device** in der Administratorkonsole nicht ausgewählt ist. [CVADHELP-16596]

Behobene Probleme in früheren Releases

Behobene Probleme in Release 20.12.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme in Release 20.11.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme in Release 20.10.5

Auf iPads und iPhones mit einer neuen Installation der Citrix Workspace-App für iOS 20.7.0 und höher schlägt das Importieren von Clientzertifikaten möglicherweise fehl. Als Ergebnis wird die folgende Fehlermeldung angezeigt.

```
Certificate cannot be imported. Error when importing into the key chain
because the certificate is not in P12 format.
```

[CVADHELP-15685]

Behobene Probleme in Release 20.10.0

In einem Cloudsetup werden Apps, die kürzlich von Citrix Workspace für iOS gestartet wurden, möglicherweise nicht für das Widget “Today” in iPhones und iPads geladen. [RFIOS-5528]

Behobene Probleme in Release 20.9.5

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme in Release 20.9.0

- In Cloud-Bereitstellungen schlägt die Anmeldung bei der Citrix Workspace-App für iOS möglicherweise fehl, wenn Azure Active Directory oder Google Identity Provider als Identitätsanbieter verwendet wird. [CVADHELP-14845]
- Wenn Sie die Citrix Workspace-App für iOS auf einem iPad im Querformat verwenden, wird die Symbolleiste auf der Seite **Einstellungen > Konto verwalten > Neues Konto hinzufügen > Manuelles Setup** nach rechts verschoben und der Link **Speichern** wird verdeckt. [CVADHELP-15376]
- In veröffentlichten Desktops wird der Berührungszeiger möglicherweise unerwartet ausgeblendet, wenn Sie eine Sitzung schließen oder minimieren und dann zu ihr zurückkehren. [CVADHELP-15354]

Behobene Probleme in Release 20.8.1

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme in Release 20.8.0

- Auf einem iOS-Gerät funktioniert die Tastenkombination STRG+UMSCHALTTASTE nicht wie erwartet. Das Problem tritt auf, wenn Sie eine externe Tastatur mit dem Gerät verbinden. [CVADHELP-15048]
- Wenn Sie eine veröffentlichte Anwendung starten, wird der Desktop Viewer-Bildschirm schwarz angezeigt und die Sitzung wird getrennt. [CVADHELP-14628]

Behobene Probleme in Release 20.7.6

- In einer Sitzung können Sie nur dann Zeichen mit einer externen Tastatur eingeben, wenn Sie in der Sitzung auf der Symbolleiste auf die Option **Tastatur** tippen. Das Problem tritt auf iOS 12.x-Geräten auf. [CVADHELP-14779]
- Wenn eine externe Tastatur an ein iOS 12.x-Gerät angeschlossen ist, werden die erweiterten Tasten nicht angezeigt, wenn Sie auf der Symbolleiste in der Sitzung auf die Option **Tastatur** tippen. [CVADHELP-14674]

Behobene Probleme in Release 20.7.5

- Versuche, eine Verbindung zu einem versteckten Store herzustellen, schlagen möglicherweise fehl, nachdem Sie die Citrix Workspace-App auf Version 20.5.0.5 aktualisiert haben. [CVADHELP-14998]

Behobene Probleme in Release 20.7.0

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Behobene Probleme in Release 20.6.0

- Beim Hinzufügen eines Webstorekontos hat die Citrix Workspace-App für iOS Zertifikatfehler ignoriert. Ab dieser Version wird eine entsprechende Fehlermeldung angezeigt, wenn Sie ein Webstore- oder ein Webinterfacekonto mit einem ungültigen Zertifikat hinzufügen. [RFIOS-5403]

Behobene Probleme in Release 20.5.0

- Das Starten von Anwendungen in der Citrix Workspace-App schlägt mit der folgenden Fehlermeldung fehl:
  "CAMAuthManErrorNoSuitableLogonProtocol"

  Das Problem tritt aufgrund einer falschen API auf. [RFIOS-5530]

Behobene Probleme in Release 20.4.5

- Wenn Sie auf einer nicht-englischen Tastatur die Anmeldeinformationen auf der Seite zum **Anmelden** eingeben, wird der Inhalt des Felds **Kennwort** auf Englisch angezeigt. [CVADHELP-14068]

Behobene Probleme in Release 20.4.0

- Die einer Doppeltipp-Geste zugewiesene Aktion funktioniert möglicherweise nicht wie erwartet. Das Problem tritt auf, wenn ein zusätzliches Tippen aus der Citrix Workspace-App eine andere Aktion ausführt. Die Doppeltipp-Aktion funktioniert ordnungsgemäß, wenn Sie die Citrix X1-Maus oder eine Bildschirmmaus verwenden. [RFIOS-4814]
- Die Bildschirmtastatur wird bei jedem Tippen angezeigt, selbst wenn sie abgedockt ist. [RFIOS-5267]
- Wenn Sie sich von einem Cloudkonto durch Tippen auf **Einstellungen** > **Store** > **Abmelden** abmelden, funktioniert der Abmeldevorgang möglicherweise nicht wie erwartet. Das Problem tritt zeitweise auf iPhones auf. [RFIOS-5197]
- Nach dem Ändern eines DNS schlägt das Starten einer Sitzung möglicherweise mit einem Verbindungsfehler fehl. Dieses Problem tritt aufgrund einer veralteten IP-Auflösung im Cache auf. [RFIOS-5358]

Behobene Probleme in Release 20.3.0

- Wenn Sie die Citrix Workspace-App in einem Cloudsetup öffnen, wird der Zählerbadge nicht aktualisiert. [RFIOS-5194]

Behobene Probleme in Release 20.2.2

- Single Sign-On ist nicht mit Citrix Files kompatibel. [RFIOS-5564]

Behobene Probleme in Release 20.2.0

- Wenn Sie in der Citrix Gateway-Sitzung auf die Schaltfläche “Zurück” tippen, werden Sie möglicherweise abgemeldet und zur Anmeldeseite geleitet. Das Problem tritt auf, wenn Sie über das Webinterface (WI) auf die Citrix Workspace-App zugreifen. [RFIOS-5059]
- Änderungen, die auf eine Bereitstellungsgruppe angewendet werden, werden möglicherweise nicht mit dem Store synchronisiert. Daher wird die Liste der Apps nicht aktualisiert. [RFIOS-5103]
- Der Zeiger der Citrix X1-Maus verschwindet möglicherweise unerwartet. Das Problem tritt auf, wenn Sie von der Citrix Workspace-App weg navigieren, während eine Sitzung aktiv oder der Bildschirm mit den Mauseinstellungen geöffnet ist, und dann zurück zur Citrix Workspace-App wechseln. [RFIOS-5349]

Behobene Probleme in Release 20.1.5

- Versuche, ein Softwaretoken zu importieren, wenn Sie auf eine `.sdtid`-Datei klicken, schlagen möglicherweise fehl. Das Problem tritt auf iOS 13.3 und iPadOS 13.3 auf. [RFIOS-5236]
- Die Citrix Workspace-App wird nach dem 1. Januar 2020 unerwartet beendet, wenn die Kamera in einer veröffentlichten Sitzung verwendet wird. Das Problem tritt nicht auf, wenn Sie das Datum manuell auf 2019 festlegen. [RFIOS-5208]
- In einem Cloudsetup zeigt der Zählerbadge möglicherweise eine falsche Zahl an. [RFIOS-5195]

Behobene Probleme in Release 20.1.0

- Versuche, einen veröffentlichten Desktop mit einem in der Cloud gehosteten VDA zu starten, schlagen möglicherweise fehl. Das Problem tritt auf, wenn der VDA aus einem ausgeschalteten Zustand startet. [RFIOS-5027]
- Versuche, Konten mit der E-Mail-basierten Kontoermittlung hinzuzufügen, schlagen möglicherweise mit der folgenden Fehlermeldung fehl:

  ```
  Cannot Add Account. Workspace cannot find the server for this domain.
  If you received a URL from your IT, you can enter that instead of your
  email.
  ```

  Das Problem tritt auf, wenn Sie von Version 1910.5 auf 1911 aktualisieren. [RFIOS-5052]

Bekannte Probleme

Bekannte Probleme in Release 21.1.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in früheren Versionen

Bekannte Probleme in Release 20.12.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.11.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.10.5

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.10.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.9.5

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.9.0

- In einem Cloudsetup werden Apps, die kürzlich von Citrix Workspace für iOS gestartet wurden, möglicherweise nicht für das Widget “Today” in iPhones und iPads geladen. [RFIOS-5528]
- Versuche, eine mit dem Safari-Webbrowser heruntergeladene ICA-Datei zu öffnen, schlagen sporadisch fehl. Dieses Problem tritt bei der Citrix Workspace-App für iOS auf, die auf Geräten mit iOS 14 ausgeführt wird. Versuchen Sie die folgenden zwei Workarounds:
  - Warten Sie einige Zeit, bevor Sie die heruntergeladene Datei öffnen (auch wenn das Symbol “Download abgeschlossen” angezeigt wird).
  - Gehen Sie zu **Einstellungen > Safari > Downloads**. Wählen Sie **Auf meinem iPad** aus, um die heruntergeladenen Dateien zu speichern.

[RFIOS-6599]

Bekannte Probleme in Release 20.8.1

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.8.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.7.6

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.7.5

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.6.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.5.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.4.5

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.4.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.3.0

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.2.2

In diesem Release wurden keine neuen bekannten Probleme festgestellt.

Bekannte Probleme in Release 20.2.0

- Wenn Sie sich von einem Cloudkonto durch Tippen auf **Einstellungen** > **Store** > **Abmelden** abmelden, funktioniert der Abmeldevorgang möglicherweise nicht wie erwartet. Das Problem tritt zeitweise auf iPhones auf. Als Workaround starten Sie die Citrix Workspace-App neu. [RFIOS-5197]
- Wenn Sie die **Storeeinstellungen** bearbeiten und speichern und dann die Änderungen durch Abbrechen der Authentifizierung verwerfen, wird das Workspace-Konto möglicherweise aus der App entfernt. Das Problem tritt in einem Cloudsetup auf. [RFIOS-5433]
- Wenn Sie in einem Cloudsetup die Kontoeinstellungen bearbeiten und speichern, reagiert die Citrix Workspace-App möglicherweise zeitweise nicht mehr. Als Workaround starten Sie die Citrix Workspace-App neu. [RFIOS-5379]

Bekannte Probleme in Release 20.1.5

- Wenn Sie die Citrix Workspace-App in einem Cloudsetup öffnen, wird der Zählerbadge nicht aktualisiert. [RFIOS-5194]
- Wenn Sie sich von einem Cloudkonto durch Tippen auf **Einstellungen** > **Store** > **Abmelden** abmelden, funktioniert der Abmeldevorgang möglicherweise nicht wie erwartet. Das Problem tritt zeitweise auf iPhones auf. Als Workaround starten Sie die Citrix Workspace-App neu. [RFIOS-5197]

Bekannte Probleme in Release 20.1.0

- In einem Cloudsetup zeigt der Zählerbadge möglicherweise eine falsche Zahl an. [RFIOS-5194]
- Bei Geräten mit iOS 13.3 zeigt der Zählerbadge möglicherweise eine falsche Zahl an. [RFIOS-5204]
- Die Option "Probieren Sie die Demo-Version aus" ist nicht verfügbar. [RFIOS-4902]

Einschränkungen

- Versuche, eine App durch Tippen auf die ICA-Datei im Download-Manager zu starten, schlagen fehl, wenn Sie den Safari-Webbrowser verwenden. Stellen Sie sicher, dass die neueste Version der Citrix Workspace-App oder Citrix Receiver für iOS (aber nicht beide) auf dem Gerät vorhanden ist, um einen erfolgreichen Start der App in Safari sicherzustellen. [RFIOS-5502]

Featurevorschau

Kunden haben die Möglichkeit, Featurevorschauen in ihren Umgebungen auszuprobieren, die nicht oder nur eingeschränkt zur Produktion verwendet werden, und zu den Featurevorschauen Feedback zu geben. Citrix akzeptiert keine Supportanfragen für Featurevorschauen, begrüßt jedoch Feedback zur Verbesserung der Features. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor.

Voraussetzungen für die Installation

October 20, 2020

Systemanforderungen und Kompatibilität

Geräteanforderungen

- Die Citrix Workspace-App für iOS Version 2009 und höher unterstützt iOS 14 und iPadOS 14.
- Die Citrix Workspace-App für iOS Version 1909 und höher unterstützt iOS 13 und iPadOS.
- Die Citrix Workspace-App für iOS Version 1808 und höher unterstützt iOS 12.
- Dieses Softwareupdate wurde für die folgenden Geräte validiert:
  - iPhone 7x-Modelle, iPhone 8x-Modelle und nur iPhone X-Modelle.
  - Alle iPad-Modelle, einschließlich iPad Pro. Ausnahmen: iPad 1 und iPad 2 werden nicht unterstützt.
- Unterstützung externer Bildschirme
  - iPhone, soweit vom iOS unterstützt.
  - iPad: Gemäß Unterstützung von iOS (nicht der ganze Bildschirm wird verwendet).

Serveranforderungen

Installieren Sie alle aktuellen Hotfixes für die Server.

- Für Verbindungen mit virtuellen Desktops und Apps unterstützt die Citrix Workspace-App für iOS Citrix StoreFront und das Webinterface.

  StoreFront:

  - StoreFront 3.6 oder höher (empfohlen). Die Citrix Workspace-App für iOS wurde für die aktuelle StoreFront-Version validiert. Unterstützte Vorversionen sind StoreFront 2.6 und höher.

    Bietet direkten Zugriff auf StoreFront-Stores. Die Citrix Workspace-App für iOS unterstützt auch vorherige Versionen von StoreFront.

    > **Hinweis:**
    >
    > In XenApp und XenDesktop 7.8 führte Citrix Unterstützung für den Framehawk Virtual Channel und 3D Pro ein. Diese Funktionalität wurde auf die Citrix Workspace-App für iOS ausgeweitet.

  - StoreFront konfiguriert mit einer Workspace für Website

    Bietet Zugriff auf StoreFront-Stores über einen Safari-Webbrowser. Benutzer müssen die ICA-Datei manuell im Browser öffnen. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie in der Dokumentation zu StoreFront.

  Webinterface:

  - Webinterface 5.4 mit Webinterface-Sites
  - Webinterface 5.4 mit XenApp und XenDesktop-Sites
  - Webinterface auf Citrix Gateway (browserbasierter Zugriff nur mit Safari)

    Sie müssen die Rewrite-Richtlinien aktivieren, die vom Citrix Gateway bereitgestellt werden.

- **Citrix Virtual Apps and Desktops**, **XenApp** und **XenDesktop** (eines der folgenden Produkte):
  - Citrix Virtual Apps and Desktops 7 1808 oder höher
  - Citrix XenDesktop 7.x oder höher
  - Citrix XenApp 7.5 und höher

Verbindungen, Zertifikate und Authentifizierung

Für Verbindungen mit StoreFront unterstützt die Citrix Workspace-App für iOS die folgenden Authentifizierungsmethoden:

	Workspace für Web mit Browsern	StoreFront Services-Site (nativ)	StoreFront XenApp- und XenDesktop-Site (nativ)	Citrix Gateway bei Workspace für Web (Browser)	Citrix Gateway bei StoreFront Services-Site (nativ)
Anonym	Ja	Ja			
Domäne	Ja	Ja	Ja	Ja*	Ja*
Domänen-Passthrough	Ja	Ja	Ja		
Sicherheitstoken				Ja*	Ja*
Zweistufige Authen-tifizierung (Domäne mit Sicherheitsto-ken)				Ja*	Ja*
SMS				Ja*	Nein
Smartcard		Ja		Ja*	Ja*
Benutzerzertifikat				Ja (Citrix Gateway Plug-In)	Ja (Citrix Gateway Plug-In)

* Nur für Workspace für Websites verfügbar und für Bereitstellungen, die Citrix Gateway mit oder ohne installiertem zugeordneten Plug-In auf dem Gerät enthalten.

Für Verbindungen mit dem Webinterface 5.4 unterstützt die Citrix Workspace-App für iOS die folgenden Authentifizierungsmethoden:

> **Hinweis:**
>
> Im Webinterface wird der Begriff “Explizit” für die Domänen- und Sicherheitstokenauthentifizierung verwendet.

	Webinterface (Browser)	Webinterface XenApp- und XenDesktop-Site	Citrix Gateway bei Webinterface (Browser)	Citrix Gateway bei Webinterface XenApp und XenDesktop-Site
Anonym	Ja			

	Webinterface (Browser)	Webinterface XenApp- und XenDesktop-Site	Citrix Gateway bei Webinterface (Browser)	Citrix Gateway bei Webinterface XenApp und XenDesktop-Site
Domäne	Ja	Ja	Ja*	
Domänen-Passthrough	Ja			
Sicherheitstoken			Ja*	
Zweistufige Authentifizierung (Domäne mit Sicherheitstoken)			Ja*	
SMS			Ja*	
Smartcard				
Benutzerzertifikat			Ja (Citrix Gateway Plug-In erforderlich)	

Zertifikate

Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway installiert ist, muss das Stammzertifikat (Root-Zertifikat) der Zertifizierungsstelle des Unternehmens auf dem Gerät installiert sein, um erfolgreich mit der Citrix Workspace-App für iOS auf Citrix Ressourcen zuzugreifen.

> **Hinweis:**
>
> Wenn das Zertifikat des Remotegateways beim Herstellen der Verbindung nicht verifiziert werden kann (da das Stammzertifikat nicht im lokalen Schlüsselspeicher vorhanden ist), wird eine Warnung zu einem nicht vertrauenswürdigen Zertifikat angezeigt. Wenn der Benutzer weiterarbeitet, wird eine Liste der Anwendungen angezeigt; die Anwendungen können jedoch nicht gestartet werden.

Manuell installiertes Zertifikat

In iOS 10.3 und höher wird einem Zertifikat, das Sie manuell in einem Profil installiert haben, nicht automatisch für SSL vertraut. Vertrauen von manuell installierten Zertifikatprofilen in iOS:

1. Stellen Sie sicher, dass das Zertifikatprofil auf dem Gerät installiert ist.
2. Navigieren Sie zu **Einstellungen** > **Allgemein** > **Info** > **Zertifikatsvertrauenseinstellungen**.

   Jedes Stammzertifikat (Root-Zertifikat), das über ein Profil installiert wurde, wird unter **Volles Vertrauen für Root-Zertifikate aktivieren** angezeigt.
3. Sie können das Vertrauen für jedes Stammzertifikat ein- und ausschalten.

Importieren von Stammzertifikaten auf iPad- und iPhone-Geräten

Erwerben Sie das Stammzertifikat des Zertifikatausstellers und senden es per E-Mail an ein E-Mail-Konto, das auf dem Gerät konfiguriert ist. Wenn Sie auf die Anlage klicken, werden Sie zum Importieren des Stammzertifikats aufgefordert.

Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden statt einzelner Serverzertifikate für jeden Server in derselben Domäne verwendet. Die Citrix Workspace-App für iOS unterstützt Zertifikate mit Platzhalterzeichen.

Zwischenzertifikate und Citrix Gateway

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Zertifikat des Citrix Gateway- oder Access Gateway-Servers angehängt werden. Weitere Informationen zu Access Gateway-Installationen finden Sie in dem Knowledge Center-Artikel CTX114146, der Ihrer Edition entspricht.

RSA SecurID-Authentifizierung wird für Secure Gateway-Konfigurationen (nur über das Webinterface) und alle unterstützten Access Gateway-Konfigurationen unterstützt.

Die Citrix Workspace-App für iOS unterstützt alle Authentifizierungsmethoden, die von Access Gateway unterstützt werden.

Richtlinie für die Überprüfung gemeinsamer Serverzertifikate

Releases der Citrix Workspace-App für iOS haben eine strengere Validierungsrichtlinie für Serverzertifikate.

> **Wichtig**
>
> Bestätigen Sie vor der Installation der Citrix Workspace-App für iOS, dass die Zertifikate auf dem Server oder Gateway wie hier beschrieben konfiguriert sind. Aufgrund folgender Ursachen können Verbindungen fehlschlagen:
>
> - Die Server- oder Gatewaykonfiguration enthält ein falsches Stammzertifikat

- Die Server- oder Gatewaykonfiguration enthält nicht alle Zwischenzertifikate
- Die Server- oder Gatewaykonfiguration enthält ein abgelaufenes oder anderweitig ungültiges Zwischenzertifikat
- Die Server- oder Gatewaykonfiguration enthält ein übergreifendes Zwischenzertifikat

Beim Validieren eines Serverzertifikats verwendet die Citrix Workspace-App für iOS jetzt **alle** Zertifikate, die vom Server oder Gateway bereitgestellt werden. Wie in früheren Releases überprüft die Citrix Workspace-App für iOS dann, ob die Zertifikate vertrauenswürdig sind. Wenn nicht alle Zertifikate vertrauenswürdig sind, schlägt die Verbindung fehl.

Diese Richtlinie ist strenger als die Zertifikatrichtlinie in Webbrowsern. Viele Webbrowser enthalten eine große Anzahl Stammzertifikate, denen sie vertrauen.

Der Server bzw. das Gateway muss mit den richtigen Zertifikaten konfiguriert sein. Sind nicht die richtigen Zertifikate vorhanden, schlägt die Verbindung mit der Citrix Workspace-App für iOS u. U. fehl.

Angenommen, ein Gateway ist mit gültigen Zertifikaten konfiguriert. Diese Konfiguration wird für Kunden empfohlen, die eine strengere Validierung benötigen. Dabei wird genau ermittelt, welches Stammzertifikat die Citrix Workspace-App für iOS verwendet:

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Beispielstammzertifikat

Die Citrix Workspace-App für iOS überprüft, ob alle Zertifikate gültig sind. Die Citrix Workspace-App für iOS überprüft ebenfalls, ob dem **Beispielstammzertifikat** bereits vertraut wird. Wenn die Citrix Workspace-App für iOS dem **Beispielstammzertifikat** nicht vertraut, schlägt die Verbindung fehl.

Wichtig

Einige Zertifizierungsstellen haben mehr als ein Stammzertifikat. Wenn Sie diese strengere Validierung benötigen, stellen Sie sicher, dass Ihre Konfiguration das entsprechende Stammzertifikat verwendet.

Zum Beispiel gibt es derzeit zwei Zertifikate:

- DigiCert oder GTE CyberTrust Global Root
- DigiCert Baltimore Root oder Baltimore CyberTrust Root

Diese Zertifikate können dieselben Serverzertifikate validieren. Auf einigen Benutzergeräten sind beide Stammzertifikate verfügbar. Auf anderen Geräten ist nur eins verfügbar (**DigiCert Baltimore Root**/**Baltimore CyberTrust Root**).

Wenn Sie **GTE CyberTrust Global Root** auf dem Gateway konfigurieren, schlagen die Citrix Workspace-App für iOS-Verbindungen auf diesen Benutzergeräten fehl. Aus der Dokumentation

der Zertifizierungsstelle erfahren Sie, welches Stammzertifikat zu verwenden ist. Beachten Sie außerdem, dass Stammzertifikate, wie alle Zertifikate, irgendwann ablaufen.

Die Citrix Workspace-App für iOS verwendet dann die beiden Zertifikate. Dann sucht Receiver nach einem Stammzertifikat auf dem Benutzergerät. Wird ein gültiges Zertifikat gefunden, das auch vertrauenswürdig ist (z. B. **Beispielstammzertifikat**), ist die Verbindung erfolgreich. Andernfalls schlägt die Verbindung fehl.

Beachten Sie, dass diese Konfiguration das von der Citrix Workspace-App für iOS benötigte Zwischenzertifikat zur Verfügung stellt, aber der Citrix Workspace-App für iOS auch die Wahl eines gültigen, vertrauenswürdigen Stammzertifikats ermöglicht.

Nehmen wir nun an, ein Gateway ist mit den folgenden Zertifikaten konfiguriert:

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Falsches Stammzertifikat

Ein Webbrowser ignoriert eventuell das falsche Stammzertifikat. Die Citrix Workspace-App für iOS ignoriert das falsche Stammzertifikat jedoch nicht und die Verbindung schlägt fehl.

Einige Zertifizierungsstellen verwenden mehr als ein Zwischenzertifikat. In diesem Fall ist das Gateway normalerweise wie folgt mit allen Zwischenzertifikaten konfiguriert, jedoch nicht mit dem Stammzertifikat:

- Beispielserverzertifikat
- Beispielzwischenzertifikat 1
- Beispielzwischenzertifikat 2

> **Wichtig**
>
> Einige Zertifizierungsstellen verwenden ein übergreifendes Zwischenzertifikat. Dies ist für Situationen vorgesehen, wenn mehr als ein Stammzertifikat vorhanden ist und ein früher ausgestelltes Stammzertifikat zur gleichen Zeit wie ein später ausgestelltes Stammzertifikat verwendet wird. In diesem Fall sind mindestens zwei Zwischenzertifikate vorhanden.

Beispielsweise hat das früher ausgestellte Stammzertifikat **Class 3 Public Primary Certification Authority** das entsprechende übergreifende Zwischenzertifikat **Verisign Class 3 Public Primary Certification Authority - G5**. Ein entsprechendes später ausgestelltes Stammzertifikat **Verisign Class 3 Public Primary Certification Authority - G5** ist ebenfalls verfügbar und es ersetzt **Class 3 Public Primary Certification Authority**. Das später ausgestellte Stammzertifikat verwendet kein übergreifendes Zwischenzertifikat.

> **Hinweis:**
>
> Das übergreifende Zwischenzertifikat und das Stammzertifikat haben den gleichen Antragstellernamen (Ausgestellt an), aber das übergreifende Zwischenzertifikat hat einen anderen Ausstteller-

> namen (Ausgestellt durch). Dadurch unterscheidet sich das übergreifende Zwischenzertifikat von einem normalen Zwischenzertifikat wie **Beispielzwischenzertifikat 2**.

Normalerweise empfiehlt sich die folgende Konfiguration ohne das Stammzertifikat und das übergreifende Zwischenzertifikat:

- Beispielserverzertifikat
- Beispielzwischenzertifikat

Konfigurieren Sie das Gateway nicht für die Verwendung des übergreifenden Zwischenzertifikats, weil die Citrix Workspace-App für iOS sonst das früher ausgestellte Stammzertifikat auswählt:

- Beispielserverzertifikat
- Beispielzwischenzertifikat
- Übergreifendes Beispielzwischenzertifikat [nicht empfohlen]

Es wird nicht empfohlen, das Gateway nur mit dem Serverzertifikat zu konfigurieren:

- Beispielserverzertifikat

In diesem Fall schlägt die Verbindung fehl, wenn die Citrix Workspace-App für iOS nicht alle Zwischenzertifikate finden kann.

Installieren und Aktualisieren

August 17, 2020

Upgrade

Führen Sie für die Aktualisierung auf die aktuelle Citrix Workspace-App einen der folgenden Schritte aus:

- Laden Sie die Citrix Workspace-App von der Seite Citrix Download herunter und installieren Sie die App, um von Citrix Receiver auf die Citrix Workspace-App zu aktualisieren.
- Aktualisieren Sie Ihre Citrix Workspace-App über den App-Store.

Informationen zu den Features in der Citrix Workspace-App für iOS finden Sie unter Citrix Workspace-App – Featurematrix.

Erste Schritte

October 20, 2020

Einrichtung

Die Citrix Workspace-App für iOS unterstützt die Konfiguration von Webinterface für die Citrix Virtual Apps-Bereitstellung. Es gibt zwei Arten von Webinterface-Sites: XenApp und XenDesktop-Sites und Citrix Virtual Apps and Desktops-Sites. Mit Webinterface-Sites können Clientgeräte eine Verbindung mit der Serverfarm herstellen. Die Authentifizierung zwischen Citrix Workspace-App für iOS und einer Webinterface-Site kann mit verschiedenen Lösungen gehandhabt werden, u. a. Citrix Secure Web Gateway.

Außerdem können Sie StoreFront für die Authentifizierungs- und Ressourcenbereitstellungsdienste für die Citrix Workspace-App für iOS konfigurieren; Sie können dann zentralisierte Unternehmensstores erstellen, die Desktops, Anwendungen und anderen Ressourcen den Benutzern bereitstellen.

Weitere Informationen zur Konfiguration von Verbindungen, einschließlich von Videos, Blogs und einem Supportforum finden Sie unter http://community.citrix.com.

Konfigurieren Sie die folgenden Komponenten in Ihrer Citrix Virtual Apps and Desktops-Bereitstellung wie hier beschrieben, bevor Benutzer auf Anwendungen zugreifen, die in der Bereitstellung ausgeführt werden.

- Ziehen Sie die folgenden Optionen in Betracht, wenn Sie Anwendungen in den Farmen veröffentlichen, um die Erfahrung für die Benutzer zu steigern, die über StoreFront-Stores auf die Anwendungen zugreifen.
  - Verwenden Sie aussagekräftige Beschreibungen für veröffentlichte Anwendungen, da diese Beschreibungen Benutzern in der Citrix Workspace-App für iOS angezeigt werden.
  - Sie können die Mobilgerätbenutzer auf veröffentlichte Anwendungen aufmerksam machen, wenn Sie die Anwendungen in der Highlightliste der Citrix Workspace-App für iOS einschließen. Wenn Sie dieser Liste Einträge in der Citrix Workspace-App für iOS hinzufügen möchten, bearbeiten Sie die Eigenschaften der Anwendungen, die auf den Servern veröffentlicht sind, und hängen Sie die Zeichenfolge KEYWORDS:Featured dem Feld “Anwendungsbeschreibung” an.
  - Zum Aktivieren des AutoAnpassen-Bildschirmmodus, bei dem die Anwendung auf die Bildschirmgröße der Mobilgeräte angepasst wird, müssen Sie die Eigenschaften der Anwendungen bearbeiten, die auf den Servern veröffentlicht sind, und die Zeichenfolge KEYWORDS:mobile dem Wert im Feld “Anwendungsbeschreibung” anhängen. Mit diesem Schlüsselwort wird auch der automatische Bildlauf für die Anwendung aktiviert.
  - Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, indem Sie die Zeichenfolge KEYWORDS:Auto an die Beschreibung anhängen, die Sie beim Veröffentlichen der Anwendung in Citrix Virtual Apps angeben. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.

- Wenn das Webinterface in der Citrix Virtual Apps and Desktops-Bereitstellung keine Website oder Citrix Virtual Apps and Desktops-Site hat, erstellen Sie eine Site. Der Name und die Erstellung der Site hängen von der installierten Webinterface-Version ab. Weitere Informationen zur Erstellung dieser Sites finden Sie im Abschnitt “Erstellen von Sites” für die relevante Version des Webinterface.

Manuelles Setup

Wenn die Citrix Workspace-App für iOS eine Verbindung mit einem Citrix Gateway herstellt, sucht die Citrix Workspace-App für iOS im Allgemeinen nach der Authentifizierung eine XenApp und XenDesktop-Site oder Citrix Virtual Apps-Website. Wenn keine Site gefunden wird, zeigt die Citrix Workspace-App für iOS einen Fehler an. Konfigurieren Sie ein Konto manuell, um diese Situation zu vermeiden, damit die Citrix Workspace-App für iOS eine Verbindung mit Citrix Gateway herstellen kann.

1. Tippen Sie oben rechts auf das Symbol Konten und tippen Sie dann auf dem Bildschirm Konten auf das Pluszeichen (+). Der Bildschirm Neues Konto wird angezeigt.
2. Tippen Sie unten links auf dem Bildschirm auf das Symbol links neben Optionen und tippen Sie dann auf Manuelles Setup. Zusätzliche Felder werden auf dem Bildschirm angezeigt.
3. Geben Sie im Feld “Adresse” die sichere URL der Site oder des Citrix Gateways an, zu der bzw. dem Sie eine Verbindung herstellen möchten (z. B. `agee.mycompany.com`).
4. Wählen Sie eine der folgenden Verbindungsoptionen. Die restlichen Felder auf dem Bildschirm werden entsprechend der Auswahl geändert.
    - Webinterface: Bei Auswahl zeigt die Citrix Workspace-App für iOS eine Citrix Virtual Apps-Website an, die einem Webbrowser ähnelt. Dies wird auch Webansicht genannt.
    - XenApp Services: Bei Auswahl sucht die Citrix Workspace-App für iOS eine bestimmte XenApp und XenDesktop-Site, für die eine Authentifizierung über Citrix Gateway nicht konfiguriert ist. Geben Sie für die zusätzlichen Optionen, die auf diesem Bildschirm angezeigt werden, die Anmeldeinformationen für die Site an.
        - <StoreFront-FQDN>: Bei mehreren Stores wird eine Liste angezeigt und der Benutzer kann den Store auswählen, der hinzugefügt wird.
        - <StoreFront-FQDN>/citrix/<Storename>: Der StoreFront-Store <Storename> wird hinzugefügt.
        - <StoreFront-FQDN>/citrix/PnAgent/config.xml: Der Standard-PNAgent-Legacystore wird hinzugefügt.
        - <StoreFront-FQDN>/citrix/<Storename>/PnAgent/config.xml: Der PNAgent-Legacystore, der <Storename> zugeordnet ist, wird hinzugefügt.
    - Citrix Gateway: Bei Auswahl stellt die Citrix Workspace-App für iOS eine Verbindung mit einer XenApp und XenDesktop-Site über einen bestimmten Citrix Gateway her. Wählen Sie in den zusätzlichen Optionen auf diesem Bildschirm die Serveredition und die Anmeldein-

formationen aus, einschließlich des ggf. erforderlichen Sicherheitstokens für die Authentifizierung.

5. Verwenden Sie für die Zertifikatssicherheit die Einstellung im Feld “Zertifikatwarnungen” ignorieren und legen Sie fest, ob eine Verbindung mit dem Server hergestellt wird, selbst wenn das Zertifikat ungültig, selbstsigniert oder abgelaufen ist. Die Standardeinstellung ist AUS.
   Wichtig: Wenn Sie diese Option aktivieren, stellen Sie sicher, dass Sie eine Verbindung mit dem richtigen Server herstellen. Citrix empfiehlt dringend, dass alle Server ein gültiges Zertifikat haben, um Benutzergeräte vor Onlinesicherheitsangriffen zu schützen. Ein sicherer Server verwendet ein SSL-Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde. Citrix unterstützt keine selbstsignierten Zertifikate und empfiehlt, dass die Zertifikatsicherheit nicht ausgelassen wird.
6. Tippen Sie auf Speichern.
7. Geben Sie den Benutzernamen und das Kennwort (oder das Token, wenn Sie die zweistufige Authentifizierung ausgewählt haben) ein und tippen Sie dann auf “Anmelden”. Der Citrix Workspace-App für iOS-Bildschirm wird angezeigt, von dem Sie auf die Desktops zugreifen und die Anwendungen hinzufügen und öffnen können.

StoreFront

> **Wichtig:**
>
> - Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App für iOS Citrix Access Gateway Enterprise Edition ab Version 9.3 und die Citrix Gateway-Versionen bis 13.
> - Die Citrix Workspace-App für iOS unterstützt nur XenApp und XenDesktop-Site auf dem Webinterface.
> - Die Citrix Workspace-App für iOS unterstützt das Starten von Sitzungen über Workspace für Web, sofern der verwendete Browser mit Workspace für Web funktioniert. Wenn die Starts nicht erfolgen, konfigurieren Sie Ihr Konto direkt über die Citrix Workspace-App für iOS. Benutzer müssen die ICA-Datei mit der Browserfunktion zum Öffnen in Workspace manuell öffnen. Weitere Informationen zu den Beschränkungen dieser Bereitstellung finden Sie in der Dokumentation zu StoreFront.

Mit StoreFront bestehen die erstellten Stores aus Diensten, die eine Authentifizierungs- und Ressourcenbereitstellungsinfrastruktur für die Citrix Workspace-App für iOS bereitstellen. Erstellen Sie Stores, die Desktops und Anwendungen von Citrix Virtual Apps and Desktops-Sites und Citrix Virtual Apps-Farmen auflisten und aggregieren und diese Ressourcen Benutzern zur Verfügung stellen.

1. Installieren und konfigurieren Sie StoreFront. Weitere Informationen finden Sie in der Dokumentation von StoreFront. Administratoren, die mehr Kontrolle wünschen, können mit einer von Citrix bereitgestellten Vorlage eine Downloadsite für die Citrix Workspace-App für iOS erstellen.

2. Stores für StoreFront konfigurieren Sie genauso wie für andere Citrix Virtual Apps and Desktops-Anwendungen. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich. Weitere Informationen finden Sie unter “Benutzerzugriffsoptionen” im StoreFront-Abschnitt der Produktdokumentation. Verwenden Sie für Mobilgeräte eine dieser Methoden:
    - Provisioningdateien: Sie können Benutzern Provisioningdateien (.cr) bereitstellen, die Verbindungsdetails für die Stores enthalten. Nach der Installation öffnen Benutzer die Datei auf dem Gerät, um die Citrix Workspace-App für iOS automatisch zu konfigurieren. Workspace für Websites bieten Benutzern standardmäßig eine Provisioningdatei für den einen Store, für den die Site konfiguriert ist. Alternativ können Sie mit der Citrix StoreFront-Verwaltungskonsole Provisioningdateien für einen oder mehrere Stores generieren und manuell an die Benutzer verteilen.
    - Manuelle Konfiguration: Sie können Benutzern die Informationen zur erforderlichen Citrix Gateway- oder Store-URL, mit der sie auf ihre Desktops und Anwendungen zugreifen können, direkt mitteilen. Für Verbindungen über Citrix Gateway benötigen Benutzer außerdem die Produktedition und erforderliche Authentifizierungsmethode. Nach der Installation geben Benutzer diese Informationen in der Citrix Workspace-App für iOS ein. Die Citrix Workspace-App fordert die Benutzer auf, sich anzumelden, falls die Verbindung erfolgreich überprüft werden konnte.
    - Automatische Konfiguration: Tippen Sie auf dem Willkommenbildschirm auf **Konto hinzufügen** und geben Sie die URL des StoreFront-Servers in das Feld “Adresse” ein. Das Konto wird beim Hinzufügen automatisch konfiguriert.

Konfigurieren von Citrix Gateway

Wenn Benutzer sich von außerhalb des internen Netzwerks verbinden (z. B. Benutzer, die eine Verbindung über das Internet oder von Remotestandorten aus herstellen), konfigurieren Sie die Authentifizierung über Citrix Gateway.

- Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App für iOS Citrix Access Gateway Enterprise Edition ab Version 9.3 und die Citrix Gateway-Versionen bis 13.

Webinterface

Zum Konfigurieren der Webinterface-Site können Benutzer mit iPhone- und iPad-Geräten Anwendungen über die Webinterface-Site und den integrierten Safari-Browser auf dem Mobilgerät starten. Konfigurieren Sie die Webinterface-Site genauso wie für andere Citrix Virtual Apps-Anwendungen. Wenn keine XenApp und XenDesktop-Site für das Mobilgerät konfiguriert ist, verwendet die Citrix Workspace-App für iOS automatisch die Webinterface-Site. Eine spezielle Konfiguration für Mobilgeräte ist nicht erforderlich.

Das Webinterface 5.x wird vom integrierten Safari-Browser unterstützt.

Starten von Anwendungen auf dem iOS-Gerät

Benutzer können sich vom Mobilgerät mit Ihren normalen Anmeldeinformationen und dem Kennwort an der Webinterface-Site anmelden.

Automatisches Provisioning für mobile Geräte

In StoreFront können Sie mit den Aufgaben “Multistore-Provisioningdatei exportieren” und “Provisioningdatei exportieren” Dateien mit Verbindungsinformationen für Stores generieren, z. B. für Citrix Gateway-Bereitstellungen und Beacons, die für Stores konfiguriert wurden. Stellen Sie diese Dateien Benutzern zur Verfügung, damit diese die Citrix Workspace-App für iOS automatisch mit den Details der Stores konfigurieren können. Benutzer können auch Citrix Workspace-App für iOS-Provisioningdateien von Workspace für Websites erhalten.

> **Wichtig:**
>
> Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden.

1. Klicken Sie auf der Windows-Startseite oder auf der Apps-Seite auf die Kachel Citrix StoreFront. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten Stores.
2. Um eine Provisioningdatei mit Details für mehrere Stores zu generieren, klicken Sie im Bereich “Aktionen” auf Multistore-Provisioningdatei exportieren und wählen Sie die Stores aus, die der Datei hinzugefügt werden sollen.
3. Klicken Sie auf “Exportieren” und speichern Sie die Provisioningdatei mit der Erweiterung `.cr` an einem geeigneten Speicherort im Netzwerk.

Benutzerzugriffsinformationen

Sie müssen den Benutzern die Citrix Workspace-App für iOS-Kontoinformationen bereitstellen, die für den Zugriff auf die gehosteten Anwendungen, Desktops und Daten benötigt werden. Sie können diese Informationen folgendermaßen bereitstellen:

- Konfigurieren der e-mail-basierten Kontenermittlung
- Bereitstellen einer Provisioningdatei für Benutzer
- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen

Konfigurieren der e-mail-basierten Kontenermittlung

Sie können die Citrix Workspace-App für iOS für die e-mail-basierte Kontenermittlung konfigurieren. Nach der Konfiguration geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration der Citrix Workspace-App für iOS ein. Die Citrix Workspace-App für iOS ermittelt auf der Basis von DNS-Dienstdatensätzen den Access Gateway- oder StoreFront-Server oder das virtuelle Endpoint Management-Gerät, der bzw. das der E-Mail-Adresse zugeordnet ist, und fordert die Benutzer zur Anmeldung auf, sodass sie auf ihre gehosteten Anwendungen, Desktops und Daten zugreifen können.

> **Hinweis:**
>
> Die e-mail-basierte Kontenermittlung wird nicht unterstützt, wenn die Citrix Workspace-App für iOS eine Verbindung zu einer Webinterface-Bereitstellung herstellt.

Bereitstellen einer Provisioningdatei für Benutzer

Sie können mit StoreFront ein Provisioningdateien erstellen, die Verbindungsdetails für Konten enthalten. Stellen Sie diese Dateien den Benutzern zur Verfügung, um eine automatische Konfiguration der Citrix Workspace-App für iOS zu ermöglichen. Nach der Installation der Citrix Workspace-App für iOS öffnen Benutzer die Datei mit der Erweiterung `.cr` auf dem Gerät, um die Citrix Workspace-App für iOS zu konfigurieren. Wenn Sie Workspace für Websites konfigurieren, können Benutzer die Citrix Workspace-App für iOS-Provisioningdateien auch von diesen Seiten abrufen.

Weitere Informationen finden Sie in der Dokumentation zu StoreFront.

Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer

Wenn Sie den Benutzern Kontoangaben für die manuelle Eingabe bereitstellen, stellen Sie sicher, dass die folgenden Informationen bereitgestellt werden, damit die Benutzer erfolgreich eine Verbindung zu den gehosteten Anwendungen und Desktops herstellen können:

- Die StoreFront-URL oder die XenApp and XenDesktop-Site mit den gehosteten Ressourcen, z. B.: `servername.company.com`.
- Stellen Sie für den Zugriff mit Citrix Gateway die Citrix Gateway-Adresse und die erforderliche Authentifizierungsmethode bereit.

Wenn ein Benutzer Angaben für ein neues Konto macht, versucht die Citrix Workspace-App für iOS, die Verbindung zu überprüfen. Im Erfolgsfall fordert die Citrix Workspace-App für iOS den Benutzer auf, sich bei dem Konto anzumelden.

Konfiguration

September 15, 2020

Speichern von Kennwörtern

In der Citrix Webinterface-Verwaltungskonsole konfigurieren Sie die Authentifizierungsmethode, damit Benutzer ihre Kennwörter speichern können. Wenn Sie das Benutzerkonto konfigurieren, wird das verschlüsselte Kennwort gespeichert, bis der Benutzer das erste Mal eine Verbindung herstellt. Beachten Sie Folgendes:

- Wenn Sie das Speichern des Kennworts aktivieren, speichert die Citrix Workspace-App für iOS das Kennwort für zukünftige Anmeldungen auf dem Gerät und fordert nicht zur Kennworteingabe auf, wenn Benutzer eine Verbindung zu Anwendungen herstellen.

  > **Hinweis:**
  >
  > Das Kennwort wird nur gespeichert, wenn Benutzer beim Erstellen eines Kontos ein Kennwort eingeben. Wenn kein Kennwort für das Konto eingegeben wird, wird kein Kennwort gespeichert, unabhängig von der Servereinstellung.

- Wenn Sie das Speichern des Kennworts deaktivieren (Standardeinstellung), fordert die Citrix Workspace-App für iOS Benutzer jedes Mal zur Kennworteingabe auf, wenn sie eine Verbindung herstellen.

> **Hinweis:**
>
> Für direkte StoreFront-Verbindungen können Kennwörter nicht gespeichert werden.

Überschreiben der Kennwortspeicherung

Wenn der Server Kennwörter speichert, können Benutzer, die eine Kennworteingabe bei der Anmeldung bevorzugen, das Speichern des Kennworts überschreiben:

- Machen Sie beim Erstellen des Kontos keine Eingabe in das Feld “Kennwort”.
- Löschen Sie beim Bearbeiten eines Kontos das Kennwort und speichern Sie das Konto.

Verwenden der Kennwortspeicherung

Die Citrix Workspace-App für iOS hat ein Feature, mit dem das Herstellen einer Verbindung optimiert wird, da Sie das Kennwort speichern können. Damit wird der zusätzliche Schritt für die Authentifizierung einer Sitzung bei jedem Öffnen der Citrix Workspace-App für iOS ausgelassen.

> **Hinweis:**
>
> Die Funktionalität zum Speichern des Kennworts untersützt das PNA-Protokoll. Der *native* StoreFront wird nicht unterstützt. Diese Funktionalität funktioniert jedoch, wenn StoreFront den *PNA-Legacymodus* aktiviert.

Konfigurieren von StoreFront

Konfigurieren von StoreFront zum Aktivieren der Kennwortspeicherung:

1. Wenn Sie einen vorhandenen Store konfigurieren, gehen Sie zu Schritt 3.
2. Zum Konfigurieren einer neuen StoreFront-Bereitstellung halten Sie sich an die bewährten Methoden, die unter Installieren, Einrichten und Deinstallieren von Citrix StoreFront beschrieben sind.
3. Öffnen Sie die Citrix StoreFront-Verwaltungskonsole. Stellen Sie sicher, dass die Basis-URL HTTPS verwendet und mit dem allgemeinen Namen übereinstimmt, der beim Generieren des SSL-Zertifikats angegeben wurde.
4. Wählen Sie den Store aus, den Sie konfigurieren möchten.
5. Klicken Sie auf **XenApp Services-Support konfigurieren**.
6. Aktivieren Sie **XenApp Services-Support**, wählen Sie den **Standardstore** (optional) aus und klicken Sie auf **OK**.
7. Navigieren Sie zur Vorlagenkonfigurationsdatei in c:\inetpub\wwwroot\Citrix\<storename>\Views\PnaConfi
8. Erstellen Sie ein Backup der Datei Config.aspx.
9. Öffnen Sie die Originaldatei Config.aspx.
10. Bearbeiten Sie die Zeile <EnableSavePassword>**false**</EnableSavePassword> und ändern Sie den Wert **false** in **true**.
11. Speichern Sie die bearbeitete Datei Config.aspx.
12. Führen Sie PowerShell auf dem StoreFront-Server mit Administratorrechten aus.
13. In der PowerShell-Konsole:

    a. cd “c:\Program Files\Citrix\Receiver StoreFront\Scripts”

    b. Geben Sie “Set-ExecutionPolicy RemoteSigned” ein

    c. Geben Sie “.\ImportModules.ps1” ein

    d. Geben Sie Folgendes ein: “Set-DSDerviceMonitorFeature –ServiceUrl” `https://localhost:443/StorefrontMonitor`

14. Bei einer StoreFront-Gruppe müssen Sie dieselben Befehle für alle Mitgliedern der Gruppe ausführen.

Konfigurieren von Citrix Gateway zum Speichern von Kennwörtern

> **Hinweis:**
>
> Diese Konfiguration verwendet Citrix Gateway-Server mit Lastausgleich.

Konfigurieren von Citrix Gateway für die Unterstützung der Kennwortspeicherung:

1. Melden Sie sich bei der Citrix Gateway-Verwaltungskonsole an.
2. Halten Sie sich an die bewährten Citrix-Methoden beim Erstellen eines Zertifikats für die virtuellen Server mit Lastausgleich.
3. Navigieren Sie auf der Registerkarte "Configuration" auf "Traffic Management -> Load Balancing -> Servers" und klicken Sie auf **Add**.
4. Geben Sie den Servernamen und die IP-Adresse des StoreFront-Servers ein.
5. Klicken Sie auf **Erstellen**. Wiederholen Sie für eine StoreFront-Gruppe Schritt 5 für alle Server in der Gruppe.
6. Navigieren Sie auf der Registerkarte "Configuration" auf **Traffic Management** > **Load Balancing** > **Monitor** und klicken Sie auf **Add**.
7. Geben Sie einen Namen für den Monitor ein. Wählen Sie als Typ **STOREFRONT**. Wählen Sie unten auf der Seite **Secure** (erforderlich, da der StoreFront-Server HTTPS verwendet).
8. Klicken Sie auf die Registerkarte **Special Parameters**. Geben Sie den vorher konfigurierten StoreFront-Namen ein, wählen Sie **Check Backed Services** und klicken Sie auf**Create**.
9. Navigieren Sie auf der Registerkarte **Configuration** auf **Traffic Management** > **Load Balancing** > **Service Groups** und klicken Sie auf **Add**.
10. Geben Sie einen Namen für die Dienstgruppe ein und legen Sie für das Protokoll **SSL** fest und klicken Sie auf **OK**.
11. Klicken Sie auf der rechten Seite des Bildschirms unter "Advanced Settings" auf **Settings**.
12. Aktivieren Sie die Client-IP und geben Sie Folgendes für den Headerwert ein: **X-Forwarded-For**. Klicken Sie dann auf **OK**.
13. Wählen Sie unter "Advanced Settings" auf der rechten Seite des Bildschirms **Monitors**. Klicken Sie auf den Pfeil und fügen Sie neue Monitore hinzu.
14. Klicken Sie auf die Schaltfläche **Add** und wählen Sie dann das Dropdownmenü **Select Monitor** aus. Eine Liste der auf dem Citrix Gateway konfigurierten Monitore wird angezeigt.

15. Klicken Sie auf das Optionsfeld neben den zuvor erstellten Monitoren und klicken Sie auf **Select** und dann auf **Bind**.
16. Wählen Sie unter “Advanced Settings” auf der rechten Seite des Bildschirms **Members** aus. Klicken Sie auf den Pfeil und fügen Sie neue Dienstgruppenmitglieder hinzu.
17. Klicken Sie auf die Schaltfläche **Add** und wählen Sie dann die Dropdownliste **Select Member** aus.
18. Aktivieren Sie das Optionsfeld **Server Based**. Eine Liste der auf dem Citrix Gateway konfigurierten Servermitglieder wird angezeigt. Klicken Sie auf die Optionsfelder neben den zuvor erstellten StoreFront-Servern.
19. Geben Sie für die Portnummer 443 und für die Hash-ID eine eindeutige Zahl ein. Klicken Sie dann auf **Create** und auf **Done**. Wenn alles richtig konfiguriert wurde, sollte **Effective State** ein grünes Licht anzeigen, d. h. das Monitoring funktioniert richtig.
20. Navigieren Sie auf “Traffic Management -> Load Balancing -> Virtual Servers” und klicken Sie auf **Add**. Geben Sie den Namen für den Server ein und wählen Sie als Protokoll **SSL**.
21. Geben Sie die IP-Adresse für den StoreFront-Lastausgleichsserver ein und klicken Sie auf **OK**.
22. Wählen Sie die Bindung **Load Balancing Virtual Server Service Group**, klicken Sie auf den Pfeil und fügen Sie die vorher erstellte Dienstgruppe hinzu. Klicken Sie zwei Mal auf **OK**.
23. Weisen Sie das für den virtuellen Lastausgleichsserver erstellte SSL-Zertifikat zu. Wählen Sie **No Server Certificate**.
24. Wählen Sie das Zertifikat des Lastausgleichsservers aus der Liste aus und klicken Sie auf **Bind**.
25. Fügen Sie das Domänenzertifikat dem Lastausgleichsserver hinzu. Klicken Sie auf **No CA certificate**.
26. Wählen Sie das Domänenzertifikat aus und klicken Sie auf **Bind**.
27. Wählen Sie auf der rechten Seite des Bildschirms **Persistence**.
28. Ändern Sie “Persistence” in **SOURCEIP** und stellen Sie das Timeout auf **20** ein. Klicken Sie auf **Save** und anschließend auf **Done**.
29. Fügen Sie den Lastausgleichsserver (wenn er noch nicht erstellt ist) dem Domänen-DNS-Server hinzu.
30. Starten Sie die Citrix Workspace-App für iOS auf dem iOS-Gerät und geben Sie die vollständige XenApp-URL ein.

Integration des Content Collaboration-Diensts

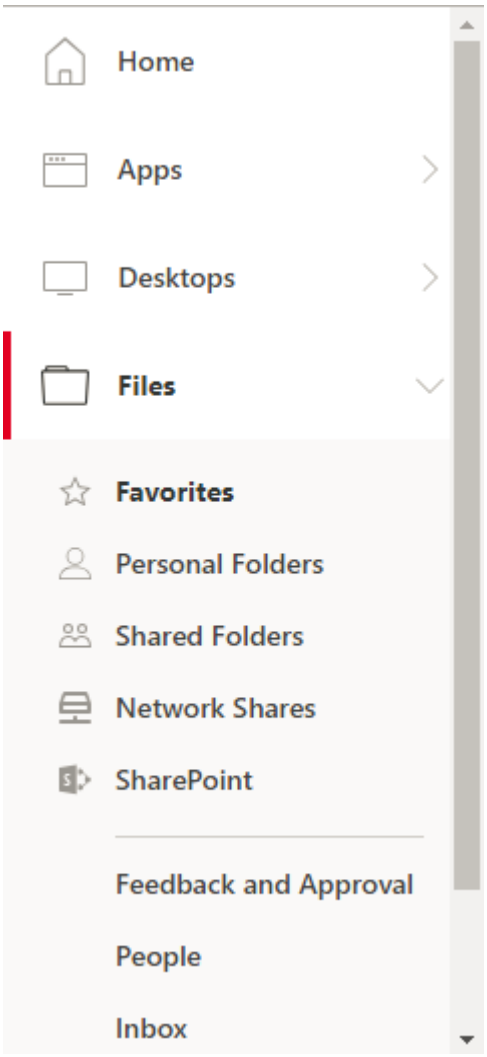
Citrix Content Collaboration ermöglicht Ihnen den einfachen und sicheren Austausch von Dokumenten, das Senden umfangreicher Dokumente per E-Mail, die sichere Übertragung von Dokumenten

an Dritte und den Zugriff auf einen Bereich für die Zusammenarbeit. Citrix Content Collaboration bietet viele Möglichkeiten zum Arbeiten, darunter eine webbasierte Benutzeroberfläche, mobile Clients, Desktop-Apps und die Integration in Microsoft Outlook und Gmail.

Sie können Citrix Content Collaboration-Funktionen über die Registerkarte Dateien der Citrix Workspace-App aufrufen. Die Registerkarte Dateien wird nur angezeigt, wenn der Content Collaboration Service in der Workspacekonfiguration der Citrix Cloud-Konsole aktiviert ist.

> **Hinweis:**
>
> Die Citrix Content Collaboration-Integration mit der Citrix Workspace-App wird unter Windows Server 2012 und Windows Server 2016 nicht unterstützt. Grund ist eine im Betriebssystem festgelegte Sicherheitsoption.

In der folgenden Abbildung sehen Sie ein Beispiel für den Inhalt der Registerkarte Dateien der neuen Citrix Workspace-App:



Einschränkungen

- Beim Zurücksetzen der Citrix Workspace-App wird Citrix Content Collaboration nicht abgemeldet.
- Durch das Wechseln von Stores in der Citrix Workspace-App wird Citrix Content Collaboration nicht abgemeldet.

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Erfasste Daten	Beschreibung	Verwendungszweck
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Workspace-App für iOS und sendet die Daten automatisch an Google Firebase.	Citrix nutzt diese Daten, um die Qualität, Zuverlässigkeit und Leistung der Workspace-App zu verbessern.

Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix und schützt sie gemäß der Anlage zur Sicherheit von Citrix Diensten, die unter Citrix Trust Center verfügbar ist.

Citrix verwendet Google Firebase, um bestimmte Daten aus der Citrix Workspace-App als Teil von CEIP zu sammeln. Bitte lesen Sie, wie Google die für Google Firebase gesammelten Daten handhabt.

Sie können das Senden von CEIP-Daten an Citrix und Google Firebase deaktivieren. Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie die Citrix Workspace-App für iOS.
2. Tippen Sie auf **Home** > **Einstellungen**.
3. Navigieren Sie zum Abschnitt **Allgemein**.
4. Deaktivieren Sie die Option **Nutzungsstatistiken senden**.

Folgende CEIP-Datenelemente werden von Google Firebase erfasst:

Sitzungsinformationen und Sitzungsstart-methode	Citrix Stores und Store-Konfiguration	Authentifizierungstyp und Authen-tifizierungskonfigura-tion	ICA-Verbindungen
HDX-Sitzungstart	Store-App-Sitzung	WebView-Aktion “Öffnen”	WebView-Aktion “Kopieren”
WebView-Aktion “Teilen”	Bewertung der Workspace-App	Verbindungsstatus, Verbindungsfehler, Connection Center-Nutzung	Externe Anzeige
Socketstatus	Sitzungsdauer	HDX über UDP	Sitzungsstartzeit
Geräteinformationen	Info zum Gerätemodell	Nutzungsstatistiken senden	App-Sprache, Workspace-App-Sprache
Sprache der Tastatur	Type des Citrix Store	Citrix Store-Kombination	Protokolltyp des Store
Store-Anzahl	HDX-UDP-Status	RSA-Tokeninstallationen	

Citrix Ready Workspace Hub

Der Citrix Ready Workspace Hub verbindet die digitale und die physische Umgebung zur Bereitstellung von Apps und Daten in einem sicheren, intelligenten Bereich. Das System verbindet Geräte (oder auch Dinge, z. B. mobile Apps und Sensoren) zur Schaffung einer intelligenten und reaktionsfähigen Umgebung.

Citrix Ready Workspace Hub baut auf der Raspberry Pi 3-Plattform auf. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, stellt eine Verbindung zum Citrix Ready Workspace Hub her und ermöglicht die Anzeige von Apps und Desktops auf einem größeren Display.

Weitere Informationen zu Citrix Ready Workspace Hub finden Sie in der Dokumentation unter Citrix Ready Workspace Hub.

Zur Sicherheit unterstützt Citrix Ready Workspace Hub eine SSL-Verbindung (Secure Sockets Layer) zwischen Mobilgeräten und dem Hub. Legen Sie einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) entweder manuell oder automatisch fest, um jedes Gerät eindeutig zu identifizieren. Weitere Informationen finden Sie unter Sichere Verbindung in der Dokumentation zu Citrix Ready Workspace Hub.

Der Citrix Ready Workspace Hub ist in der Citrix Workspace-App aktiviert, wenn alle folgenden Systemanforderungen erfüllt sind:

- Citrix Workspace-App für iOS 1810.1 oder höher
- Bluetooth aktiviert
- Mobilgerät und Workspace Hub verwenden dasselbe WLAN-Netzwerk

Konfigurieren

Um die Citrix Ready Workspace Hub-Features zu aktivieren, navigieren Sie zu **Einstellungen** und tippen Sie auf **Citrix Casting**, damit das Feature auf Ihrem Gerät verfügbar ist. Weitere Informationen finden Sie in der Hilfedokumentation zu den iOS-Geräten.

Die Citrix Workspace-App integriert ein neues Verfahren zum Hinzufügen oder Entfernen eines Workspace Hubs aus der Liste vertrauenswürdiger Geräte auf iOS-Geräten. Weitere Informationen finden Sie unter Sichere Verbindung.

Bekannte Einschränkung

- In VDA 7.18 und früheren Versionen erfordert das Casting auf einen Workspace Hub, dass für den verwendeten Desktop oder die verwendete Ressource die .h264-Vollbildrichtlinie aktiviert und die Richtlinie für Legacygrafiken deaktiviert ist.

Sitzungsfreigabe

Wenn sich Benutzer von einem Citrix Workspace-App für iOS-Konto abmelden und noch Verbindungen mit Anwendungen oder Desktops bestehen, können sie die Verbindung trennen oder sich abmelden:

- **Trennen:** Abmelden vom Konto; die Windows-Anwendung bzw. der -Desktop wird weiter auf dem Server ausgeführt. Der Benutzer kann dann ein anderes Gerät starten, die Citrix Workspace-App für iOS öffnen und sich mit dem letzten Zustand wiederverbinden, bevor er die Verbindung mit dem iOS-Gerät trennte. Mit dieser Option können sich Benutzer von einem Gerät mit einem anderen Gerät wiederverbinden und in den ausgeführten Anwendungen weiterarbeiten.
- **Abmelden:** Abmelden vom Konto; die Windows-Anwendung wird geschlossen und das Konto wird vom Citrix Virtual Apps and Desktops-Server abgemeldet. Mit dieser Option können Benutzer die Verbindung zum Server trennen und sich vom Konto abmelden. Wenn sie die Citrix Workspace App für iOS erneut starten, wird sie im Standardzustand geöffnet.

Der intelligente Workspace

Ab dem Release 1911 ist die App optimiert und in der Lage, die Vorteile der intelligenten Features zu nutzen, wenn sie veröffentlicht werden. Weitere Informationen finden Sie unter Intelligente Workspace-Funktionen - Mikroapps.

Unterstützung für iOS 13 und iPadOS

Die Citrix Workspace-App für iOS wird unter iOS 13 und iPadOS unterstützt, einschließlich Multitasking-Unterstützung für iPadOS.

> **Wichtig:**
>
> - Die CR01-App wird unter iOS 13 nicht unterstützt. Wenn Sie die CR01-App verwenden, empfiehlt Citrix, kein Upgrade auf iOS 13 durchzuführen.
> - Wenn Sie die SHA-1-Zertifikatkette verwenden, müssen Sie möglicherweise zur SHA-2-Zertifikatkette wechseln. Mit SHA-1 signierte Zertifikate gelten unter iOS 13 nicht mehr als vertrauenswürdig. Weitere Informationen zu TLS-Serverzertifikaten finden Sie unter Anforderungen für vertrauenswürdige Zertifikate in iOS 13 und macOS 10.15.
> - In iOS 13 hat sich das Starten von Sitzungen über den Safari-Webbrowser geändert. Weitere Informationen siehe Hilfe.

Die Citrix Workspace-App für iOS bietet jetzt Unterstützung für AssistiveTouch und verbindet sich nun anders mit der Citrix X1-Maus. Die Citrix Workspace-App stellt beim Start keine Verbindung mehr mit der Citrix X1-Maus her. Daher ist das Citrix X1-Maussymbol nicht mehr in der Symbolleiste neben dem Symbol “Einstellungen” verfügbar. Um zu sehen, ob der Zugriff auf eine gekoppelte Citrix X1-Maus für die Citrix Workspace-App aktiviert ist, navigieren Sie zu **Einstellungen** > **Citrix X1-Maus**.

Sitzungsroaming auf iPads

Ab Release 1906 ist Sitzungsroaming auf iPhone- und iPad Touch-Geräten verfügbar, wenn Sie einen Cloudspeicher verwenden. Weitere Informationen finden Sie in der Hilfedokumentation für iOS-Geräte.

Tastaturlayoutsynchronisierung

Die Tastaturlayoutsynchronisierung ermöglicht es Benutzern, zu bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Diese Funktion ist in der Standardeinstellung deaktiviert.

Um die Synchronisierung des Tastaturlayouts zu aktivieren, gehen Sie zu **Einstellungen** > **Tastaturoptionen** und aktivieren Sie die Option **Synchronisierung des Tastaturlayouts**.

> **Hinweis:**
>
> Wenn Sie die lokale Tastaturlayoutoption verwenden, wird der Client-IME (Eingabemethoden-Editor) aktiviert. Wenn Sie Japanisch, Chinesisch oder Koreanisch verwenden und den Server-IME bevorzugen, deaktivieren Sie die Option für das lokale Tastaturlayout, indem Sie die entsprechende Option unter **Einstellungen** > **Tastatur** deaktivieren.

Host-zu-Client-Umleitung

Bei der Inhaltsumleitung können Sie steuern, wie die Benutzer auf die Informationen zugreifen: über die auf den Servern veröffentlichten Anwendungen oder über lokal auf den Benutzergeräten ausgeführte Anwendungen.

Host-zu-Client-Umleitung ist eine Art der Inhaltsumleitung. Sie wird nur auf Serverbetriebssystem-VDAs (nicht auf Desktopbetriebssystem-VDAs) unterstützt.

Wenn die Host-zu-Client-Umleitung aktiviert ist, werden URLs auf dem Server-VDA abgefangen und an das Benutzergerät gesendet. Die URLs werden im Webbrowser oder Multimedia-Player auf dem Benutzergerät geöffnet. Wenn Sie die Host-zu-Client-Umleitung aktivieren und ein Benutzergerät keine Verbindung zu einer URL herstellen kann, wird die URL an den Server-VDA zurückgeleitet. Ist die Host-zu-Client-Umleitung deaktiviert, öffnen die Benutzer die URLs mit Webbrowsern oder Multimedia-Playern auf dem Server-VDA.
Wenn Sie die Host-zu-Client-Umleitung aktivieren, können Benutzer sie nicht deaktivieren.

Die Host-zu-Client-Umleitung wurde früher Server-zu-Client-Umleitung genannt.

Weitere Informationen finden Sie unter Allgemeine Inhaltsumleitung.

Unterstützung für die Verwendung abgeleiteter Anmeldeinformationen mit Purebred

Ab Release 1810 bietet die Citrix Workspace-App für iOS Unterstützung für die Verwendung abgeleiteter Anmeldeinformationen mit Purebred. Beim Herstellen einer Verbindung mit einem Store, der abgeleitete Anmeldeinformationen zulässt, können sich Benutzer mithilfe einer virtuellen Smartcard bei der Citrix Workspace-App für iOS anmelden. Dieses Feature wird nur bei On-Premises-Bereitstellungen unterstützt.

> **Hinweis:**
>
> Citrix Virtual Apps and Desktops 7 1808 oder höher ist für dieses Feature erforderlich.

Weitere Informationen zum Konfigurieren von abgeleiteten Anmeldeinformationen finden Sie unter Abgeleitete Anmeldeinformationen.

Authentifizierung

August 17, 2020

Clientzertifikatauthentifizierung

> **Wichtig:**
>
> - Bei Verwendung von StoreFront unterstützt die Citrix Workspace-App für iOS Folgendes:
>   - Citrix Access Gateway Enterprise Edition Version 9.3
>   - NetScaler Gateway Version 10.x bis Version 11.0
>   - Citrix Gateway Version 11.1 und höher
> - Die Clientzertifikatauthentifizierung wird von der Citrix Workspace-App für iOS unterstützt.
> - Nur Access Gateway Enterprise Edition 9.x und 10.x (und spätere Releases) unterstützen die Clientzertifikatauthentifizierung.
> - Die Zweiquellenauthentifizierungstypen müssen CERT und LDAP sein.
> - Die Citrix Workspace-App für iOS unterstützt die optionale Clientzertifikatauthentifizierung.
> - Nur Zertifikate im P12-Format werden unterstützt.

Benutzer, die sich an einem virtuellen Citrix Gateway-Server anmelden, können auch anhand der Attribute des Clientzertifikats authentifiziert werden, das dem virtuellen Server präsentiert wird. Die Clientzertifikatauthentifizierung kann zusammen mit einem anderen Authentifizierungstyp, LDAP, verwendet werden, um eine Zweiquellenauthentifizierung bereitzustellen.

Um Benutzer basierend auf Clientzertifikatattributen zu authentifizieren, sollte die Clientauthentifizierung auf dem virtuellen Server aktiviert sein und das Clientzertifikat angefordert werden. Sie müssen ein Stammzertifikat an den virtuellen Server von Citrix Gateway binden.

Wenn sich Benutzer am virtuellen Citrix Gateway-Server anmelden, werden nach der Authentifizierung die Informationen zum Benutzernamen und der Domäne aus dem angegebenen Feld des Zertifikats extrahiert. Diese Informationen müssen im Feld es Zertifikats **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** enthalten sein. Das Format ist “Benutzername@Domäne”. Wenn der Benutzername und die Domäne extrahiert wurden und der Benutzer die anderen benötigten Informationen (beispielsweise ein Kennwort) eingibt, ist der Benutzer authentifiziert. Wenn der Benutzer kein gültiges Zertifikat und keine gültigen Anmeldeinformationen bereitstellt oder wenn der Benutzername bzw. die Domäne nicht extrahiert werden kann, schlägt die Authentifizierung fehl.

Sie können Benutzer anhand des Clientzertifikats authentifizieren, indem Sie für den Standardauthentifizierungstyp die Verwendung des Clientzertifikats angeben. Sie können auch eine Zertifikataktion erstellen, mit der Sie definieren, was während der Authentifizierung basierend auf einem Client-SSL-Zertifikat geschehen soll.

Konfigurieren der XenApp Services-Site

Wenn keine XenApp Services-Site vorhanden ist, erstellen Sie eine XenApp Services-Site für Mobilgeräte in der Citrix Virtual Apps-Konsole oder der Webinterface-Konsole (abhängig von der installierten Citrix Virtual Apps-Version).

Die Citrix Workspace-App für iOS für Mobilgeräte ruft über eine XenApp Services-Site Informationen zu den Anwendungen ab, für die ein Benutzer Berechtigungen hat, und bietet sie der App an, die auf dem Gerät ausgeführt wird. Dies gleicht der Weise, wie das Webinterface für traditionelle SSL-basierte Citrix Virtual Apps-Verbindungen, für die ein Citrix Gateway konfiguriert werden kann, verwendet wird.

Konfigurieren Sie die XenApp Services-Site für die Citrix Workspace-App für iOS für Mobilgeräte, um Verbindungen von einer Citrix Gateway-Verbindung zu ermöglichen.

1. Wählen Sie in der XenApp Services-Site **Manage secure client access > Edit secure client access settings**.
2. Ändern Sie die Zugriffsmethode in Gateway Direct.
3. Geben Sie den FQDN des Citrix Gateway-Geräts ein.
4. Geben Sie die Secure Ticket Authority (STA)-Informationen ein.

Konfigurieren des Citrix Gateway-Geräts

Konfigurieren Sie das Citrix Gateway für die Clientzertifikatauthentifizierung mit der zweistufigen Authentifizierung und den zwei Authentifizierungsrichtlinien: Cert und LDAP.

1. Erstellen Sie eine Sitzungsrichtlinie auf dem Citrix Gateway, um eingehende Citrix Virtual Apps-Verbindungen von der Citrix Workspace-App für iOS zuzulassen, und geben Sie den Speicherort der neu erstellten XenApp Services-Site an.

    - Erstellen Sie eine Sitzungsrichtlinie, mit der Sie angeben, dass die Verbindung von der Citrix Workspace-App für iOS für Mobilgeräte ist. Konfigurieren Sie bei der Erstellung der Sitzungsrichtlinie den folgenden Ausdruck und wählen Sie Match All Expressions als Operator aus:

      REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace

    - Stellen Sie in der zugeordneten Profilkonfiguration für die Sitzungsrichtlinie auf der Registerkarte Security den Eintrag Default Authorization auf Allow.

      Wenn dies auf der Registerkarte “Published Applications” keine globale Einstellung ist (das Kontrollkästchen “Override Global” ist aktiviert), stellen Sie sicher, dass das Feld “ICA-Proxy” auf ON eingestellt ist.

      Geben Sie im Feld für die Webinterface-Adresse die URL mit der Datei config.xml für die XenApp Services-Site ein, die Gerätebenutzer verwenden, beispielsweise //XenAppServer-

Name/Citrix/PNAgent/config.xml oder /XenAppServerName/benutzerdefinierterPfad/-config.xml.

- Binden Sie die Sitzungsrichtlinie an den virtuellen Server.
- Erstellen Sie Authentifizierungsrichtlinien für Cert und LDAP.
- Binden Sie die Authentifizierungsrichtlinien an den virtuellen Server.
- Konfigurieren Sie den virtuellen Server so, dass Clientzertifikate im TLS-Handshake angefordert werden. Öffnen Sie dafür auf der Registerkarte Certificate die Option SSL-Parameters und stellen Sie für die Clientauthentifizierung Client Certificate auf Mandatory.

> **Wichtig:**
>
> Wenn das auf dem Citrix Gateway verwendete Serverzertifikat Teil einer Zertifikatskette ist (mit einem Zwischenzertifikat), stellen Sie sicher, dass die Zwischenzertifikate auch richtig auf dem Citrix Gateway installiert werden. Weitere Informationen zur Installation von Zertifikaten finden Sie in der Citrix Gateway-Dokumentation.

Konfigurieren des Mobilgeräts

Wenn die Clientzertifikatauthentifizierung in Citrix Gateway aktiviert ist, werden Benutzer basierend auf bestimmten Attributen des Clientzertifikats authentifiziert. Nach dem Abschluss der Authentifizierung werden der Benutzername und die Domäne aus dem Zertifikat extrahiert und alle für den Benutzer angegebenen Richtlinien angewendet.

1. Öffnen Sie in der Citrix Workspace-App für iOS das Konto und geben Sie im Feld "Server" den entsprechenden FQDN des Citrix Gateway-Servers ein, z. B. GatewayClientCertificate-Server.organization.com. Die Citrix Workspace-App für iOS erkennt automatisch, dass das Clientzertifikat benötigt wird.
2. Benutzer können entweder ein neues Zertifikat installieren oder eines aus der Liste der bereits installierten Zertifikate auswählen. Für die iOS-Clientzertifikatauthentifizierung muss das Zertifikat heruntergeladen und nur von der Citrix Workspace-App für iOS installiert werden.
3. Nach der Auswahl eines gültigen Zertifikats werden in den Feldern für den Benutzernamen und die Domäne auf dem Anmeldebildschirm der Benutzername vom Zertifikat angezeigt; Benutzer geben die restlichen Angaben ein, u. a. das Kennwort.
4. Wenn die Clientzertifikatauthentifizierung optional ist, können Benutzer die Zertifikatauswahl überspringen, wenn sie auf der Zertifikatseite auf "Back" klicken. In diesem Fall stellt die Citrix Workspace-App für iOS die Verbindung her und zeigt dem Benutzer einen Anmeldebildschirm.
5. Nachdem Benutzer die Erstanmeldung abgeschlossen haben, können sie Anwendungen ohne erneute Angabe des Zertifikats starten. Die Citrix Workspace-App für iOS speichert das Zertifikat für das Konto und verwendet es automatisch für weitere Anmeldungen.

Smartcards

Die Citrix Workspace-App für iOS bietet Unterstützung für SITHS-Smartcards, jedoch nur für Verbindungen innerhalb von Sitzungen.

Wenn Sie FIPS Citrix Gateway-Geräte verwenden, sollten Sie die Systeme so konfigurieren, dass SSL-Neuaushandlungen abgelehnt werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX123680.

Die folgenden Produkte und Konfigurationen werden unterstützt:

- Unterstützte Smartcardleser:
  - Precise Biometrics Tactivo für iPad Mini Firmwareversion 3.8.0
  - Precise Biometrics Tactivo für iPad (4. Generation) und Tactivo für iPad (3. Generation) und iPad 2 Firmwareversion 3.8.0
  - BaiMobile® 301MP und 301MP-L Smartcardleser
- Unterstützte VDA-Smartcard-Middleware
  - ActiveIdentity
- Unterstützte Smartcards:
  - PIV-Karten
  - Common Access Card (CAC)
- Unterstützte Konfigurationen:
  - Smartcardauthentifizierung bei Citrix Gateway mit StoreFront 2.x und XenDesktop 7.x und höher oder XenApp 6.5 und höher

Konfigurieren der Citrix Workspace-App für iOS für den Zugriff auf Anwendungen

1. Wenn Sie die Citrix Workspace-App für iOS so konfigurieren möchten, dass Receiver automatisch beim Erstellen eines Kontos auf Apps zugreift, geben Sie im Feld “Adresse” die entsprechende URL des Stores ein, beispielsweise storefront.organisation.com oder netscalervserver.organisation.com.
2. Wählen Sie die Option **Smartcard verwenden**, wenn Sie die Authentifizierung mit Smartcard durchführen.

> **Hinweis:**
>
> Anmeldungen am Store sind für etwa eine Stunde gültig. Anschließend müssen Benutzer sich neu anmelden, um die Darstellung zu aktualisieren oder andere Anwendungen zu starten.

RSA SecurID-Authentifizierung

RSA SecurID-Authentifizierung für die Citrix Workspace-App für iOS wird für Secure Web Gateway-Konfigurationen (nur über das Webinterface) und alle Citrix Gateway-Konfigurationen unterstützt.

Für den Softwaretoken auf der Citrix Workspace-App für iOS benötigtes URL-Schema: Der RSA SecurID-Softwaretoken, der von der Citrix Workspace-App für iOS verwendet wird, registriert nur das URL-Schema com.citrix.securid.

Wenn Benutzer die Citrix Workspace-App für iOS-Anwendung und die RSA SecurID-Anwendung auf dem iOS-Gerät installiert haben, müssen Benutzer das URL-Schema "com.citrix.securid" auswählen, um den RSA SecurID-Softwareauthentifikator (Softwaretoken) in der Citrix Workspace-App für iOS auf den Geräten zu installieren.

Importieren eines RSA SecurID-Softwaretokens

Für die Verwendung eines RSA-Softwaretokens mit der Citrix Workspace-App für iOS müssen Benutzer folgende Schritte ausführen.

Die Richtlinie für die PIN-Länge, den Typ der PIN (nur nummerisch, alphanumerisch) und die Einschränkungen für die PIN-Wiederverwendung werden auf dem RSA-Verwaltungsserver festgelegt.

Die Benutzer sollten dies nur einmal tun müssen, wenn sie sich am RSA-Server erfolgreich authentifiziert haben. Nach der Überprüfung der PINs werden die Benutzer auch am StoreFront-Server authentifiziert, und er zeigt verfügbare veröffentlichte Anwendungen und Desktops an.

Verwenden eines RSA-Softwaretoken

1. Importieren Sie den RSA-Softwaretoken, den Ihre Organisation bereitgestellt hat.
2. Wählen Sie in der E-Mail mit der angehängten SecurID-Datei **In Workspace öffnen** als Importzielort aus. Nach dem Import des Softwaretokens wird die Citrix Workspace-App für iOS automatisch geöffnet.
3. Falls Ihre Organisation ein Kennwort für den Abschluss des Imports bereitgestellt hat, geben Sie das bereitgestellte Kennwort ein und klicken Sie auf **OK**. Nach dem Klicken auf **OK** gibt eine Meldung den erfolgreichen Import des Tokens an.
4. Schließen Sie die Importmeldung und klicken Sie in der Citrix Workspace-App für iOS auf **Konto hinzufügen**.
5. Geben Sie die URL des von der Organisation bereitgestellten Stores ein und klicken Sie auf **Weiter**.
6. Geben Sie auf dem Anmeldebildschirm Ihre Anmeldeinformationen ein: Benutzername, Kennwort und Domäne. Geben Sie im Feld "PIN" **0000** ein, wenn Ihnen keine andere Standard-PIN bereitgestellt wurde. (Die PIN 0000 ist ein RSA-Standard; Ihre Organisation hat sie ggf. geändert, um eigene Sicherheitsrichtlinien einzuhalten.)
7. Klicken Sie oben links auf **Anmelden**. Nach dem Klicken auf **Anmelden** werden Sie zum Erstellen einer neuen PIN aufgefordert.

8. Geben Sie eine PIN mit 4 bis 8 Stellen ein und klicken Sie auf **OK**.
9. Sie müssen die neue PIN dann bestätigen. Geben Sie Ihre PIN erneut ein und klicken Sie auf **OK**. Nach dem Klicken Auf “OK” können Sie auf die Apps und Desktops zugreifen.

Nächster Tokencode

Wenn Sie Citrix Gateway für die RSA SecurID-Authentifizierung konfigurieren, unterstützt die Citrix Workspace-App für iOS “Nächster Tokencode”. Wenn dieses Feature aktiviert ist und ein Benutzer drei (Standardwert) falsche Kennwörter eingibt, fordert das Citrix Gateway Plug-In den Benutzer auf, so lange mit der Anmeldung zu warten, bis das nächste Token aktiv ist. Der RSA-Server kann so konfiguriert werden, dass das Konto eines Benutzers, der sich zu oft mit einem falschen Kennwort anmeldet, deaktiviert wird.

Abgeleitete Anmeldeinformationen

Unterstützung für die Verwendung abgeleiteter Anmeldeinformationen mit Purebred in der Citrix Workspace App für iOS ist verfügbar. Beim Herstellen einer Verbindung mit einem Store, der abgeleitete Anmeldeinformationen zulässt, können sich Benutzer mithilfe einer virtuellen Smartcard bei der Citrix Workspace-App für iOS anmelden. Dieses Feature wird nur bei On-Premises-Bereitstellungen unterstützt.

> **Hinweis:**
>
> Citrix Virtual Apps and Desktops 7 1808 oder höher ist für dieses Feature erforderlich.

Aktivieren von abgeleiteten Anmeldeinformationen in der Citrix Workspace-App für iOS:

1. Navigieren Sie zu **Einstellungen > Erweitert > Abgeleitete Anmeldeinformationen**.
2. Tippen Sie auf **Abgeleitete Anmeldeinformationen verwenden**.

Mit folgenden Schritten erstellen Sie anschließend eine virtuelle Smartcard, die mit abgeleiteten Anmeldeinformationen verwendet werden kann:

1. Tippen Sie unter **Einstellungen > Erweitert > Abgeleitete Anmeldeinformationen** auf **Neue virtuelle Smartcard hinzufügen**.
2. Bearbeiten Sie den Namen der virtuellen Smartcard.
3. Geben Sie eine 8-stellige PIN ein (nur Zahlen) und bestätigen Sie sie.
4. Tippen Sie auf **Weiter**.
5. Tippen Sie unter “Authentifizierungszertifikat” auf **Zertifikat importieren…**
6. Das Dokumentauswahlfenster wird angezeigt. Tippen Sie auf **Durchsuchen**.
7. Tippen Sie unter “Speicherort” auf **Purebred Key Chain**.
8. Wählen Sie das gewünschte Authentifizierungszertifikat in der Liste aus.
9. Tippen Sie auf **Schlüssel importieren**.

10. Wiederholen Sie ggf. die Schritte 5 bis 9 für das digitale Signaturzertifikat und das Verschlüsselungszertifikat.
11. Tippen Sie auf **Speichern**.

Sie können bis zu drei Zertifikate für Ihre virtuelle Smartcard importieren. Das Authentifizierungszertifikat ist erforderlich, damit die virtuelle Smartcard ordnungsgemäß funktioniert. Das Verschlüsselungszertifikat und das digitale Signaturzertifikat können zur Verwendung innerhalb einer VDA-Sitzung hinzugefügt werden.

> **Hinweis:**
>
> Beim Herstellen einer Verbindung zu einer HDX-Sitzung wird die erstellte virtuelle Smartcard in die Sitzung umgeleitet.

Bekannte Einschränkungen

- Benutzer können jeweils nur eine aktive Karte haben.
- Wenn eine virtuelle Smartcard erstellt wurde, kann sie nicht mehr bearbeitet werden. Um Änderungen an der virtuellen Smartcard vorzunehmen, müssen Benutzer die Karte löschen und eine neue Karte erstellen.
- Sie haben bis zu 10 Eingabeversuche für eine PIN. Nach dem 10. Versuch wird die virtuelle Smartcard gelöscht.
- Wenn abgeleitete Anmeldeinformationen ausgewählt werden, überschreibt die zuvor erstellte virtuelle Smartcard eine physische Smartcard, wenn eine Smartcard in einer Sitzung benötigt wird.

Sicherheit

August 17, 2020

Zum Sichern der Kommunikation zwischen der Serverfarm und der Citrix Workspace-App für iOS können Sie Verbindungen zur Serverfarm mit zahlreichen Sicherheitsverfahren integrieren, einschließlich Citrix Gateway.

> **Hinweis:**
>
> Citrix empfiehlt das Schützen der Kommunikation zwischen StoreFront-Servern und Benutzergeräten mit Citrix Gateway.

- Ein SOCKS-Proxyserver oder sicherer Proxyserver (auch Sicherheitsproxyserver, HTTPS-Proxyserver). Mit Proxyservern schränken Sie den Zugriff auf das Netzwerk und vom Netzwerk ein und handhaben Verbindungen zwischen der Citrix Workspace-App für iOS und Servern. Die Citrix Workspace-App für iOS unterstützt die Protokolle SOCKS und Secure Proxy.

- Secure Web Gateway. Secure Web Gateway stellt zusammen mit dem Webinterface einen einzigen sicheren, verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereit.
- SSL-Relay-Lösungen mit Transport Layer Security (TLS)-Protokollen.
- Eine Firewall. Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie die Citrix Workspace-App für iOS mit einer Firewall verwenden, die die interne Netzwerk-IP-Adresse des Servers einer externen Internetadresse zuweist (d. h. Netzwerkadressübersetzung oder NAT), konfigurieren Sie die externe Adresse.

Citrix Gateway

Damit Remotebenutzer sich mit der Citrix Endpoint Management-Bereitstellung über Citrix Gateway verbinden können, konfigurieren Sie Zertifikate für StoreFront. Die Methode für das Aktivieren des Zugriffs hängt von der in der Bereitstellung verwendeten Citrix Endpoint Management-Edition ab.

Wenn Sie Citrix Endpoint Management im Netzwerk bereitstellen, lassen Sie Verbindungen von internen oder Remotebenutzern mit StoreFront über Citrix Gateway zu, indem Sie Citrix Gateway und StoreFront integrieren. In dieser Bereitstellung verbinden sich Benutzer mit StoreFront und greifen auf von XenApp veröffentliche Anwendungen und auf von XenDesktop virtualisierte Desktops zu. Benutzer stellen eine Verbindung über die Citrix Workspace-App für iOS her.

Secure Web Gateway

Dieser Abschnitt gilt nur für Bereitstellungen mit dem Webinterface.

Sie können das Secure Web Gateway im Modus Normal oder Relay verwenden, um einen sicheren Kommunikationskanal zwischen der Citrix Workspace-App für iOS und dem Server bereitzustellen. Die Citrix Workspace-App für iOS muss nicht konfiguriert werden, wenn Sie das Secure Web Gateway im Normalmodus verwenden und Benutzer eine Verbindung über das Webinterface herstellen.

Für Verbindungen mit Secure Web Gateway-Servern verwendet die Citrix Workspace-App für iOS Einstellungen, die remote auf dem Webinterface-Server konfiguriert wurden.

Wenn der Secure Web Gateway Proxy auf einem Server im sicheren Netzwerk installiert ist, können Sie den Secure Web Gateway Proxy im Relaymodus verwenden. Wenn Sie den Relaymodus verwenden, fungiert der Secure Web Gateway-Server als Proxy und Sie müssen die Citrix Workspace-App für iOS für die Verwendung konfigurieren:

- Vollqualifizierter Domänenname (FQDN) des Secure Web Gateway-Servers.
- Portnummer des Secure Web Gateway-Servers. Der Relaymodus wird von Secure Web Gateway Version 2.0 nicht unterstützt.

Der FQDN muss der Reihe nach die folgenden Komponenten auflisten:

- Hostname
- Second-Level-Domäne
- Top-Level-Domäne

Beispiel: `my_computer.example.com` ist ein vollqualifizierter Domänenname, da er – in der richtigen Reihenfolge – einen Hostnamen (`my_computer`), eine Second-Level-Domäne (example) und eine Top-Level-Domäne (`com`) auflistet. Die Kombination von Second-Level- und Top-Level-Domäne (`example. com`) wird als Domänenname bezeichnet.

Proxyserver

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und Verbindungen zwischen der Citrix Workspace-App für iOS und Servern gehandhabt. Die Citrix Workspace-App für iOS unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem Citrix Virtual Apps and Desktops-Server verwendet die Citrix Workspace-App für iOS die Proxyservereinstellungen, die remote auf dem Webinterface-Server konfiguriert sind.

Für die Kommunikation mit dem Webserver verwendet die Citrix Workspace-App für iOS die Proxyservereinstellungen, die für den Standardwebbrowser auf dem Benutzergerät konfiguriert sind. Sie müssen die Proxyservereinstellungen für den Standardwebbrowser entsprechend auf dem Benutzergerät konfigurieren.

Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall in der Bereitstellung verwenden, muss die Citrix Workspace-App für iOS über die Firewall mit dem Webserver und dem Citrix Server kommunizieren können. Die Firewall muss HTTP-Datenübertragungen für die Kommunikation zwischen Benutzergerät und Webserver zulassen (meist über den HTTP-Standardport 80 oder 443, wenn ein sicherer Webserver verwendet wird). Für die Kommunikation mit dem Citrix-Server muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen.

Wenn die Firewall für die Netzwerkadressenübersetzung konfiguriert ist, definieren Sie im Webinterface Zuordnungen von internen Adressen zu externen Adressen und Ports. Beispiel: Wenn der Citrix Virtual Apps and Desktops-Server nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface der Citrix Workspace-App für iOS eine alternative Adresse bereitstellen. Die Citrix Workspace-App für iOS stellt dann mit der externen Adresse und der Portnummer eine Verbindung mit dem Server her.

TLS

Die Citrix Workspace-App für iOS unterstützt TLS 1.0, 1.1 und 1.2 mit den folgenden Verschlüsselungssammlungen für TLS-Verbindungen mit XenApp und XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Hinweis:**
>
> Die Citrix Workspace-App für iOS, die auf iOS 9 und höher ausgeführt wird, unterstützt nicht die folgenden TLS-Verschlüsselungssammlungen:
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

TLS (Transport Layer Security) ist die neueste, standardisierte Version des TLS-Protokolls. Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von TLS als offenem Standard übernahm.

TLS sichert die Datenkommunikation mit Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfen der Nachrichtenintegrität. Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie z. B. FIPS 140. FIPS 140 ist ein Standard für die Kryptografie.

Die Citrix Workspace-App für iOS unterstützt RSA-Schlüssellängen von 1024, 2048 und 3072 Bits. Darüber hinaus werden Stammzertifikate mit RSA-Schlüsseln von 4096 Bits Länge unterstützt.

> **Hinweis:**
>
> Die Citrix Workspace-App für iOS verwendet plattformeigene Kryptografie (iOS) für Verbindungen zwischen der Citrix Workspace-App für iOS und StoreFront.

Konfigurieren und Aktivieren von TLS

Das Setup von TLS besteht aus zwei Hauptschritten:

1. Setup von SSL-Relay auf dem Citrix Virtual Apps and Desktops-Server und dem Webinterface-Server und Abrufen und Installieren des benötigten Serverzertifikats.
2. Installieren Sie das entsprechende Stammzertifikat auf dem Benutzergerät.

Installieren von Stammzertifikaten auf Benutzergeräten

Für das Sichern der Kommunikation mit TLS zwischen TLS-aktivierter Citrix Workspace-App für iOS und Citrix Virtual Apps and Desktops muss auf dem Clientgerät ein Stammzertifikat vorhanden sein, mit dem die Signatur der Zertifizierungsstelle für das Serverzertifikat bestätigt wird.

iOS hat ungefähr 100 installierte kommerzielle Stammzertifikate; wenn Sie ein anderes Zertifikat verwenden möchten, rufen Sie es von einer Zertifizierungsstelle ab und installieren Sie es auf allen Benutzergeräten.

Abhängig von den Richtlinien und Abläufen in Ihrem Unternehmen möchten Sie das Stammzertifikat ggf. auf jedem Benutzergerät installieren und die Installation nicht den Benutzern überlassen. Am einfachsten und sichersten ist es, wenn Sie die Stammzertifikate der iOS-Schlüsselkette hinzufügen.

Hinzufügen eines Stammzertifikats zur Schlüsselkette

1. Senden Sie sich selbst eine E-Mail mit der Zertifikatdatei.
2. Öffnen Sie die Zertifikatdatei auf dem Gerät. Die Anwendung für den Schlüsselkettenzugriff wird automatisch gestartet.
3. Folgen Sie die Anweisungen, um das Zertifikat hinzuzufügen.
4. Ab iOS 10 stellen Sie in den iOS-Einstellungen unter “Allgemein > Info > Zertifikatvertrauenseinstellungen” sicher, dass das Zertifikat als vertrauenswürdig angesehen wird. Überprüfen Sie unter “Zertifikatvertrauenseinstellungen” den Abschnitt “VOLLES VERTRAUEN FÜR ROOT-ZERTIFIKATE AKTIVIEREN”. Stellen Sie sicher, dass für Ihr Zertifikat volles Vertrauen aktiviert ist.

Das Stammzertifikat ist installiert und kann von TLS-fähigen Clients und anderen Anwendungen, die TLS einsetzen, verwendet werden.

XenApp und XenDesktop-Site

So konfigurieren Sie die XenApp und XenDesktop-Site:

> **Wichtig:**
>
> - Citrix Secure Gateway 3.x wird von der Citrix Workspace-App für iOS mit XenApp und XenDesktop-Sites unterstützt.
> - Citrix Secure Gateway 3.x wird von der Citrix Workspace-App für iOS mit Citrix Virtual Apps-Websites unterstützt.
> - Nur einstufige Authentifizierung wird für XenApp und XenDesktop-Sites unterstützt; einstufige und zweistufige Authentifizierung werden für Citrix Virtual Apps-Websites unterstützt.
> - Sie müssen Webinterface 5.4 verwenden, das von allen integrierten Browsern unterstützt wird.

Installieren und konfigurieren Sie Citrix Gateway für die Verwendung mit dem Webinterface, bevor Sie mit dieser Konfiguration beginnen. Sie können diese Anweisungen an ihre spezifische Umgebung anpassen.

Wenn Sie eine Citrix Secure Gateway-Verbindung verwenden, konfigurieren Sie keine Citrix Gateway-Einstellungen auf der Citrix Workspace-App für iOS.

Die Citrix Workspace-App für iOS ruft über eine XenApp und XenDesktop-Site Informationen über die Anwendungen ab, für die ein Benutzer berechtigt ist und bietet sie der Citrix Workspace-App für iOS an, die auf dem Gerät ausgeführt wird. Dies gleicht der Weise, wie das Webinterface für traditionelle SSL-basierte Citrix Virtual Apps-Verbindungen, für die ein Citrix Gateway konfiguriert werden kann, verwendet wird. Diese Konfiguration ist in XenApp und XenDesktop-Sites integriert, die auf einem Server mit dem Webinterface 5.x ausgeführt werden.

Konfigurieren Sie die XenApp und XenDesktop-Site, um Verbindungen von einer Citrix Secure Gateway-Verbindung zu unterstützen.

1. Wählen Sie in der XenApp und XenDesktop-Site “Sicheren Clientzugriff verwalten” > “Einstellungen für sicheren Clientzugriff verwalten”.
2. Ändern Sie die Zugriffsmethode in Gateway Direct.
3. Geben Sie den FQDN von Secure Web Gateway ein.
4. Geben Sie die Secure Ticket Authority (STA)-Informationen ein.

> **Hinweis:**
>
> Citrix empfiehlt, für Citrix Secure Gateway den Citrix Standardpfad für diese Site zu verwenden (//XenAppServerName/Citrix/PNAgent). Mit dem Standardpfad können Benutzer den FQDN von Secure Web Gateway angeben, zu dem Sie eine Verbindung herstellen, anstatt des vollständigen Pfads zu der Datei config.xml, die sich auf der XenApp und XenDesktop-Site befindet (z. B. //XenAppServerName/CustomPath/config.xml).

Konfigurieren von Citrix Secure Gateway

1. Verwenden Sie den Citrix Secure Gateway-Konfigurationsassistenten, um Citrix Secure Gateway für die Verwendung mit dem Server im sicheren Netzwerk, der die XenApp Services-Site hostet, zu konfigurieren. Nachdem Sie die Option “Indirect” ausgewählt haben, geben Sie den FQDN-Pfad Ihres Secure Web Gateway-Servers ein und setzen Sie den Assistenten fort.
2. Testen Sie eine Verbindung von einem Benutzergerät aus, um sicherzustellen, dass Netzwerk und Zertifikatzuteilung für Secure Web Gateway richtig konfiguriert sind.

Konfigurieren des Mobilgeräts

1. Geben Sie beim Hinzufügen eines Citrix Secure Gateway-Kontos den FQDN des Citrix Secure Gateway-Servers in das Feld **Adresse** ein:

- Wenn Sie die XenApp und XenDesktop-Site mit dem Standardpfad (/Citrix/PNAgent) erstellt haben, geben Sie den Secure Web Gateway-FQDN ein: SecureGatewayFQDN.Unternehmen.com.
- Wenn Sie den Pfad der XenApp und XenDesktop-Site angepasst haben, geben Sie den vollständigen Pfad zur Datei config.xml an, z. B.: SecureGatewayFQDN.Unternehmen.com/Benutzerdefinie

2. Wenn Sie das Konto manuell konfigurieren, deaktivieren Sie die Citrix Gateway-Option **Neues Konto**.

Problembehandlung

August 17, 2020

Getrennte Sitzungen

Benutzer können eine Citrix Workspace-App für iOS-Sitzung wie folgt trennen (kein Abmelden):

- Beim Anzeigen einer veröffentlichten App oder einem veröffentlichten Desktop in einer Sitzung:
  - Tippen Sie auf den Pfeil oben auf dem Bildschirm, um das Dropdownmenü in der Sitzung anzuzeigen.
  - Tippen Sie auf die Schaltfläche **Home**, um zum Launchpad zurückzukehren.
  - Achten Sie auf den weißen Schatten unter dem Symbol einer der veröffentlichten Apps, die noch in einer aktiven Sitzung sind; tippen Sie auf das Symbol.
  - Tippen Sie auf “Trennen”.
- Schließen der Citrix Workspace-App für iOS:
  - Tippen Sie zweimal auf die Schaltfläche **Home** des Geräts.
  - Suchen Sie die Citrix Workspace-App für iOS im iOS App Switcher.
  - Tippen Sie im angezeigten Dialogfeld auf “Trennen”.
- Drücken Sie die Home-Taste auf dem Mobilgerät.
- Tippen Sie auf “Home” oder “Wechseln” im Dropdownmenü der App.

Die Sitzung bleibt im getrennten Zustand. Benutzer können sich mit dieser Sitzung später wieder verbinden. Administratoren können aber auch sicherstellen, dass getrennte Sitzungen nach einem bestimmten Zeitraum deaktiviert werden. Hierfür konfigurieren Sie ein Sitzungstimeout für die ICA-tcp-Verbindung in der Konfiguration des Remotedesktop-Sitzungsserverhosts (früher “Terminaldienstekonfiguration” genannt). Weitere Informationen zur Konfiguration von Remotedesktopdiensten (früher “Terminaldienste” genannt) finden Sie in der Produktdokumentation für Microsoft Windows Server.

Abgelaufene Kennwörter

Die Citrix Workspace-App für iOS unterstützt das benutzerseitige Ändern abgelaufener Kennwörter. Benutzer werden zur Eingabe der benötigten Informationen aufgefordert.

Geräte mit Jailbreak

Benutzer können die Sicherheit der Bereitstellung kompromittieren, wenn sie Verbindungen mit iOS-Geräten mit Jailbreak herstellen. Geräte mit Jailbreak wurden von ihren Besitzern modifiziert, wodurch meistens bestimmte Sicherheitsfunktionen umgangen werden.

Wenn die Citrix Workspace-App für iOS ein iOS-Gerät mit Jailbreak erkennt, wird der Benutzer mit einer angezeigten Warnung darauf hingewiesen. Zur weiteren Sicherung der Umgebung können Sie StoreFront oder das Webinterface so konfigurieren, dass Geräte mit erkanntem Jailbreak keine Apps ausführen können.

Anforderungen

- Citrix Receiver für iOS 6.1 oder höher
- StoreFront 3.0 oder Webinterface 5.4 oder höher
- Zugriff auf StoreFront oder das Webinterface mit einem Administratorkonto

Verhindern, dass Geräte mit erkanntem Jailbreak Apps ausführen

1. Melden Sie sich am StoreFront- oder Webinterface-Server als ein Benutzer mit Administratorrechten an.
2. Suchen Sie die Datei default.ica, die in einem der folgenden Verzeichnisse gespeichert ist:
    - **C:\inetpub\wwwroot\Citrix***storename***conf** (Microsoft-Internetinformationsdienste)
    - **C:\inetpub\wwwroot\Citrix***storename***App_Data** (Microsoft-Internetinformationsdienste)
    - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. Fügen Sie unter dem Abschnitt **[Application]** Folgendes hinzu: **AllowJailBrokenDevices=OFF**
4. Speichern Sie die Datei und starten Sie den StoreFront- oder Webinterface-Server neu.

Nach dem Neustart des StoreFront-Servers können Benutzer, denen die Warnung zu Geräten mit Jailbreak angezeigt wird, keine Apps vom StoreFront- oder Webinterface-Server starten.

Zulassen, dass Geräte mit erkanntem Jailbreak Apps ausführen

Wenn Sie AllowJailBrokenDevices nicht einstellen, wird die Warnmeldung standardmäßig den Benutzern von Geräten mit Jailbreak angezeigt; die Benutzer können die Anwendungen jedoch starten.

So lassen Sie ausdrücklich zu, dass Benutzer Anwendungen auf Geräten mit Jailbreak ausführen können:

1. Melden Sie sich am StoreFront- oder Webinterface-Server als ein Benutzer mit Administratorrechten an.
2. Suchen Sie die Datei default.ica, die in einem der folgenden Verzeichnisse gespeichert ist:
   - **C:\inetpub\wwwroot\Citrix***storename***conf** (Microsoft-Internetinformationsdienste)
   - **C:\inetpub\wwwroot\Citrix***storename***App_Data** (Microsoft-Internetinformationsdienste)
   - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. Fügen Sie unter dem Abschnitt **[Application]** Folgendes hinzu: **AllowJailBrokenDevices=ON**
4. Speichern Sie die Datei und starten Sie den StoreFront- oder Webinterface-Server neu.

Wenn Sie AllowJailBrokenDevices auf ON setzen, wird den Benutzern die Warnung zur Verwendung eines Geräts mit Jailbreak angezeigt, sie können jedoch Anwendungen über StoreFront- oder das Webinterface ausführen.

Verlust der HDX-Audioqualität

Von Citrix Virtual Apps and Desktops kann die Qualität von HDX-Audio zur Citrix Workspace-App für iOS reduziert sein, wenn Audio und Video gleichzeitig verwendet wird. Das Problem tritt auf, wenn die Citrix Virtual Apps and Desktops-HDX-Richtlinien die Audiodatenmenge zusammen mit den Videodaten nicht handhaben können. Empfehlungen zum Erstellen von Richtlinien für eine verbesserte Audioqualität finden Sie im Knowledge Center-Artikel CTX123543.

Zifferntasten und Sonderzeichen

Wenn Zifferntasten oder chinesische IME-Zeichen nicht ordnungsgemäß funktionieren, deaktivieren Sie die Unicode-Tastaturoption. Gehen Sie dazu zu **Einstellungen** > **Tastaturoptionen** und stellen Sie **Unicode-Tastatur verwenden** auf “Aus”.

Langsame Verbindungen

Wenn die Verbindung mit der XenApp und XenDesktop-Site langsam ist oder Probleme wie fehlende Programmsymbole oder Meldungen zu “Protokolltreiberfehler” auftreten, können Sie als Workaround auf dem Citrix Virtual Apps-Server und Citrix Secure Web Gateway oder dem Webinterface-Server die folgenden Citrix PV-Ethernetadapter-Eigenschaften für die Netzwerkkarte deaktivieren (alle Eigenschaften sind standardmäßig aktiviert):

- Large Send Offload
- Offload IP Checksum

- Offload TCP Checksum
- Offload UDP Checksum

Ein Serverneustart ist nicht erforderlich. Dieser Workaround gilt für Windows Server 2003 und 2008 (32 Bit). Bei Windows Server 2008 R2 tritt das Problem nicht auf.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States